Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste

I Semestre 2023

Lecture 1: Introduction and Course Logistic

Who I am

Assistant-professor (tenure-track)
DIA, Università degli Studi di Trieste

Master in Mathematics, Phd in Computer Science
Research in Formal Verification applied to Artificial Intelligence
Lot of about Runtime Verification and Temporal Logics

Office c3 2.55
Mail: lnenzi@units.it

Course Logistics

Room: aula TB Fisica tecnica - ed. C5

Timing

- Monday 17:00-18:30
- Wednesday 13:15-14:00 (13:30-15:00)
- Friday 12:00-13:30

- Some seminars

Course Website

Moodle

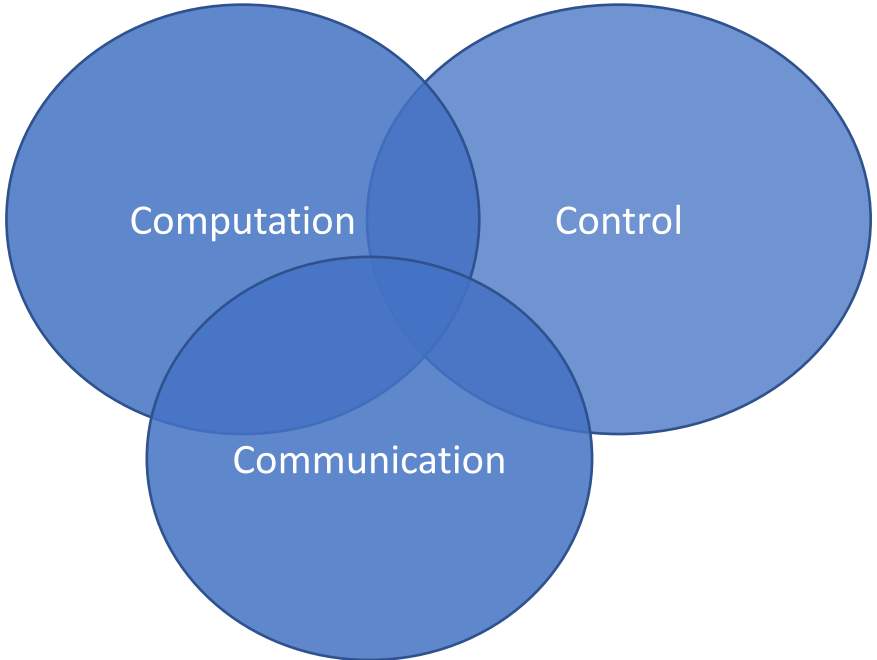
Teams

What is a Cyber-Physical System?

A CPS is a **mechanism** that is controlled or monitored by **computer-based algorithms**, tightly integrated with the Internet and its users.

Physical = physical device or system + environment

Cyber = computational + communicational

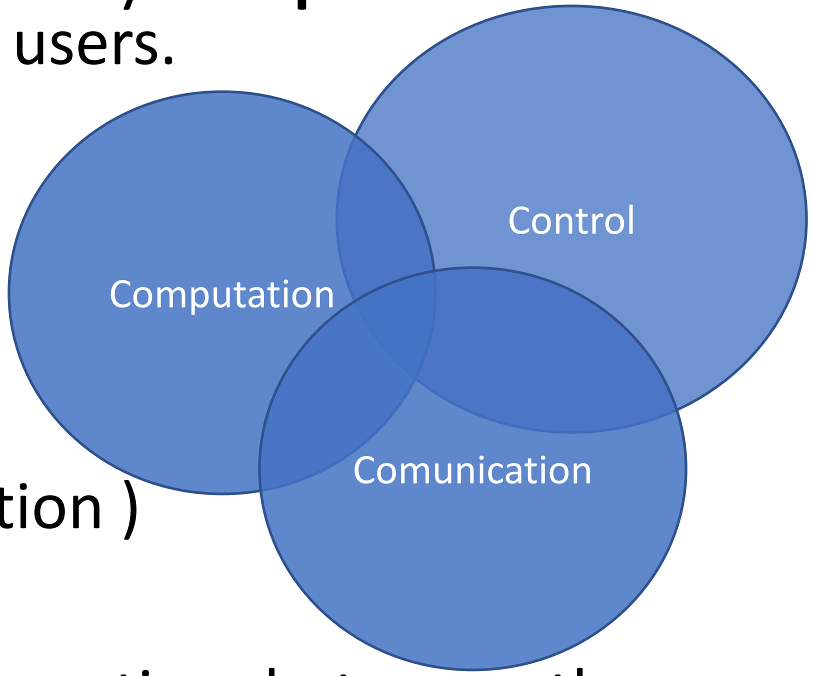


What is a Cyber-Physical System?

A CPS is a **mechanism** that is controlled or monitored by **computer-based algorithms**, tightly integrated with the Internet and its users.

Physical = physical device or system + environment

Cyber = computational + communicational



Coined in 2006 by Helen Gill (National Science Foundation)

The important part in CPS is the conjunction/intersection between the computing part and physical dynamics

What is a Cyber-Physical System?

In cyber-physical systems, physical and software components are:

- **deeply intertwined**
- each operating on **different spatial and temporal scale**
- exhibiting **multiple and distinct behavioral modalities**
- interacting with each **other in a lot of ways** that change with context.

CPS combines elements of cybernetics, mechatronics, control theory, process science, embedded systems, distributed control, and more recently communication.

Is the Field of Cyber-Physical Systems New?

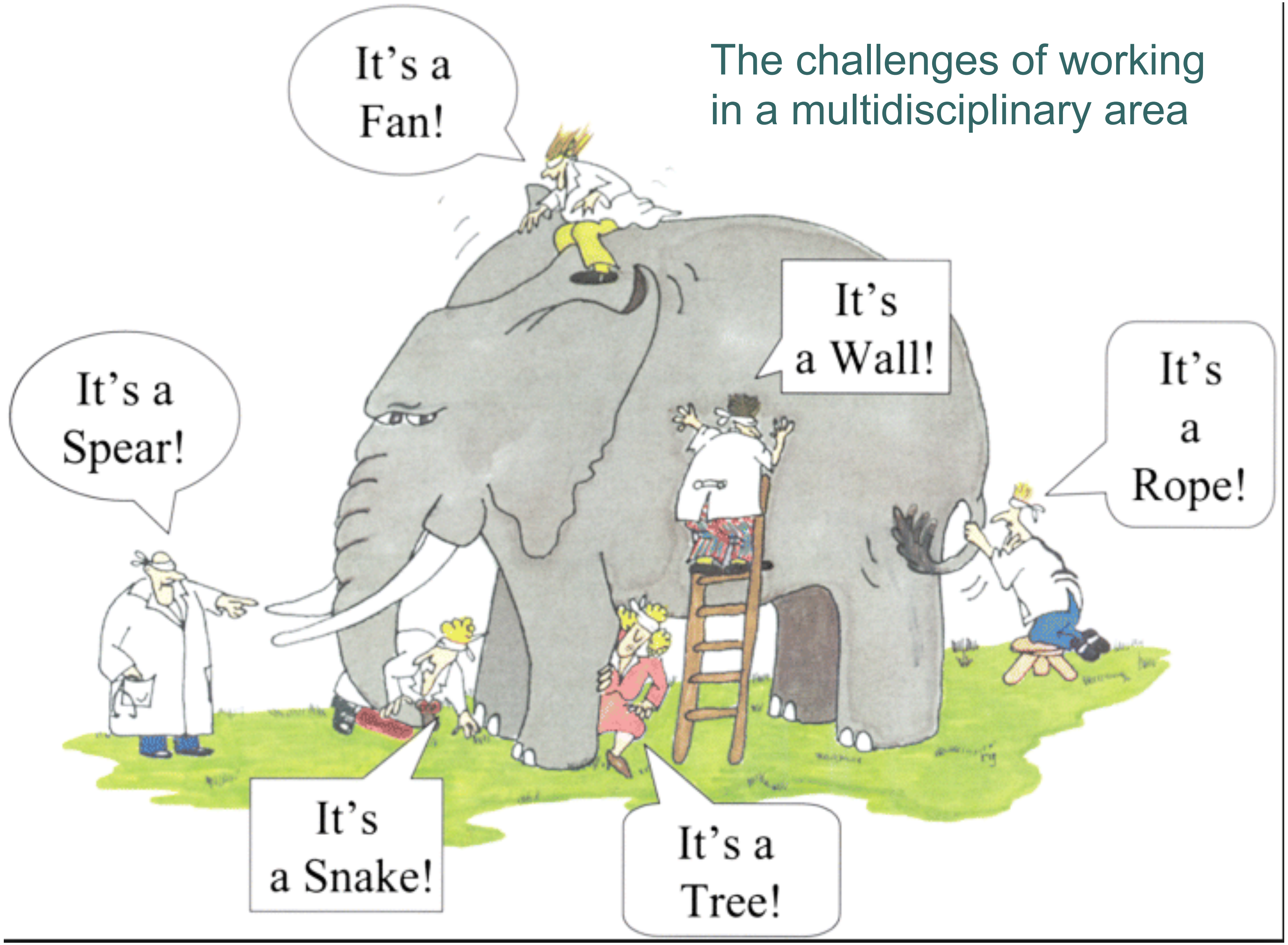
- **Hybrid Systems**: are a mathematical abstraction, CPS are real-world objects.

- **Embedded Systems**: are computational system embedded in a physical system. Any CPS contains an embedded system.

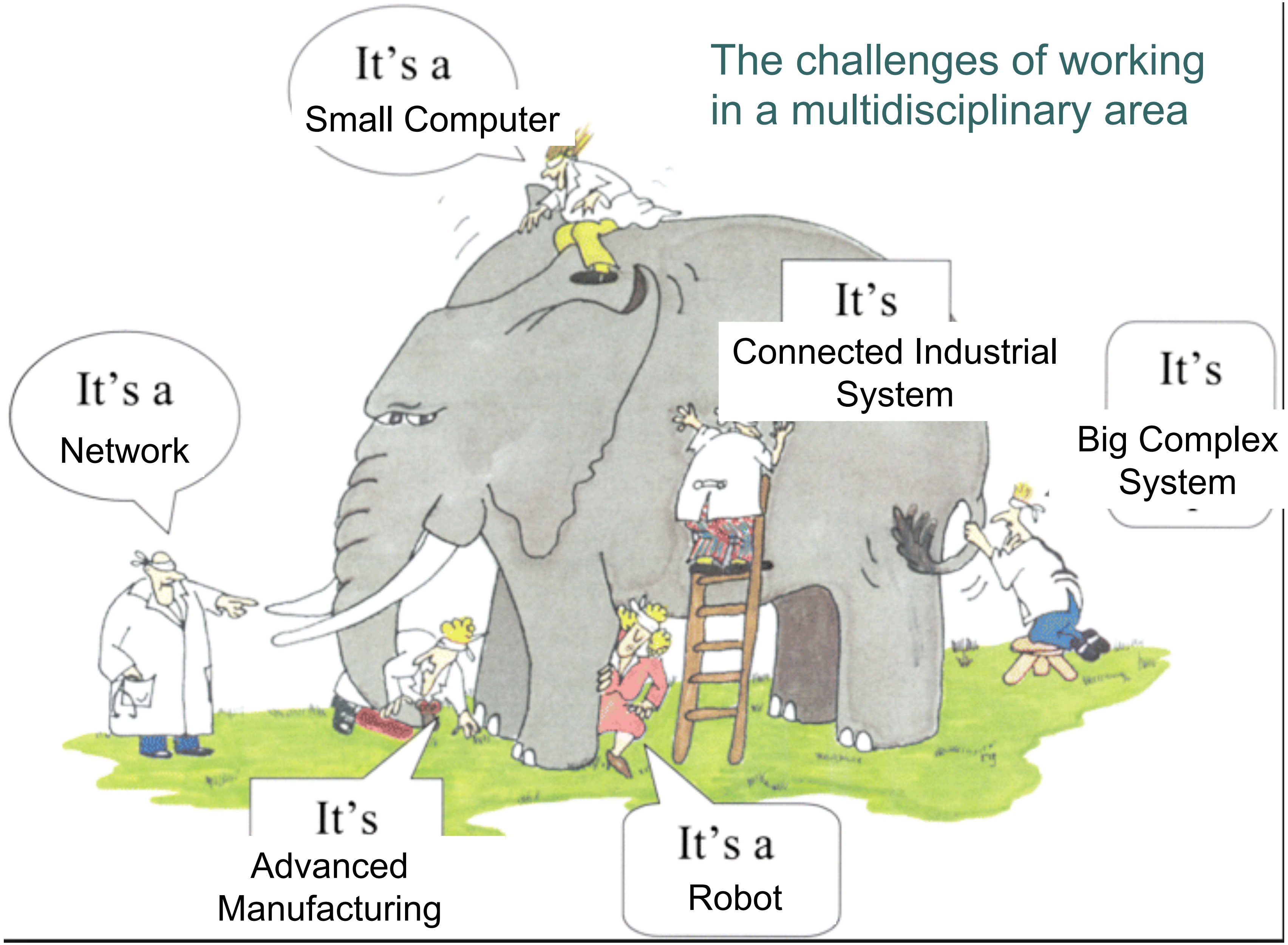
- **Real-time Systems**: must respond to external changes within certain timing constraints. Control systems can have or not real-time constraints.

- Other related disciplines: reliability, multi-agent system, mechanotronics, control theory, robotics, Internet of Things (IoT).

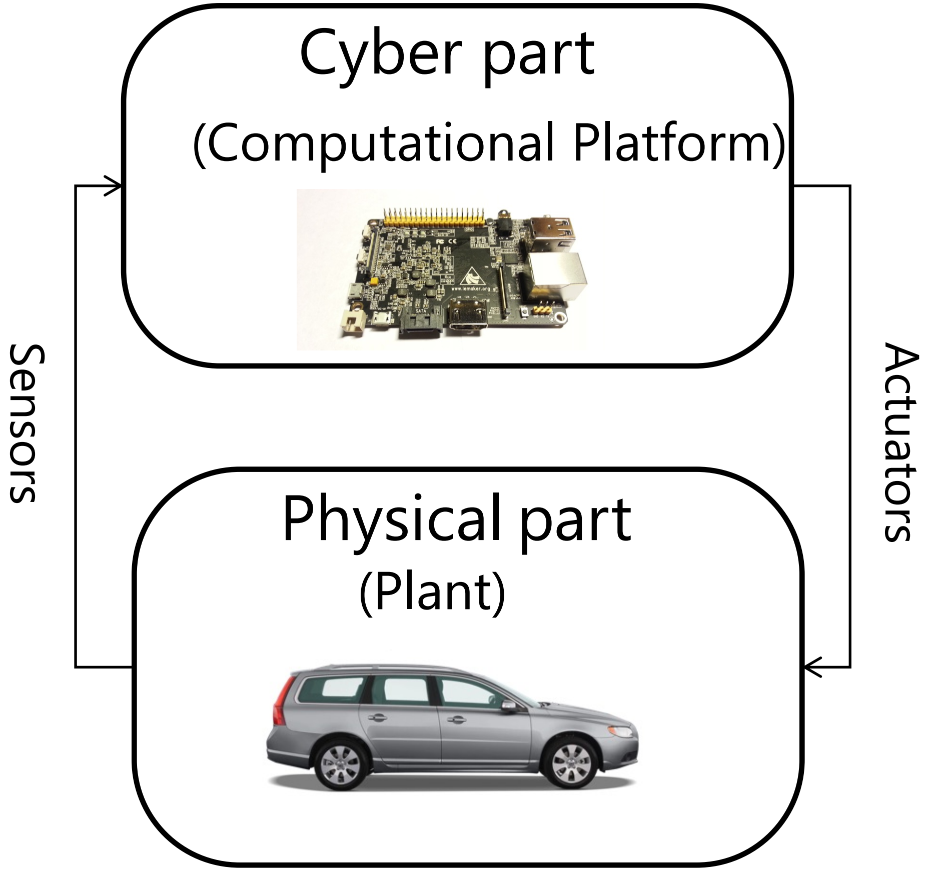
The challenges of working in a multidisciplinary area



The challenges of working in a multidisciplinary area



Example Structure of a CPS



Cyber part

(Computational Platform)

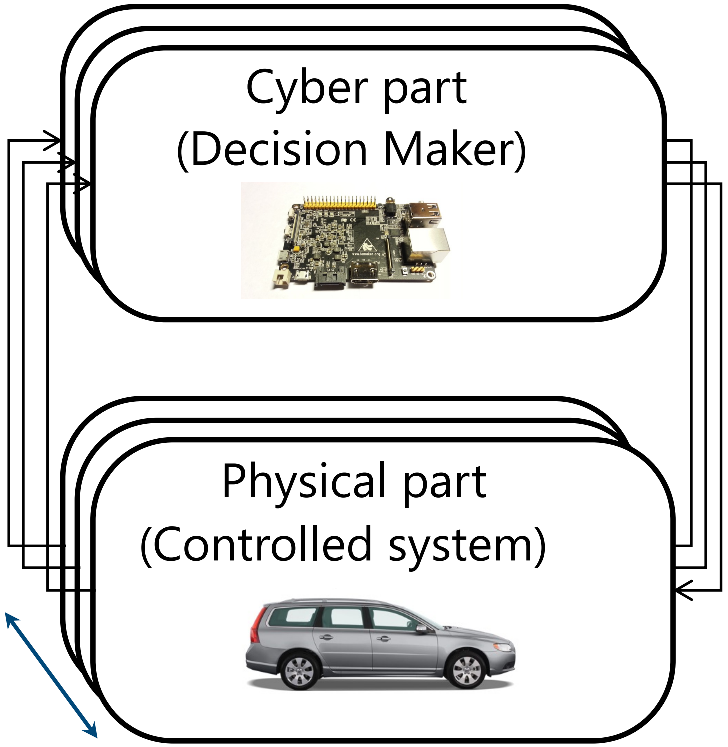
Sensors

Actuators

Physical part

(Plant)

Example Structure of a CPS

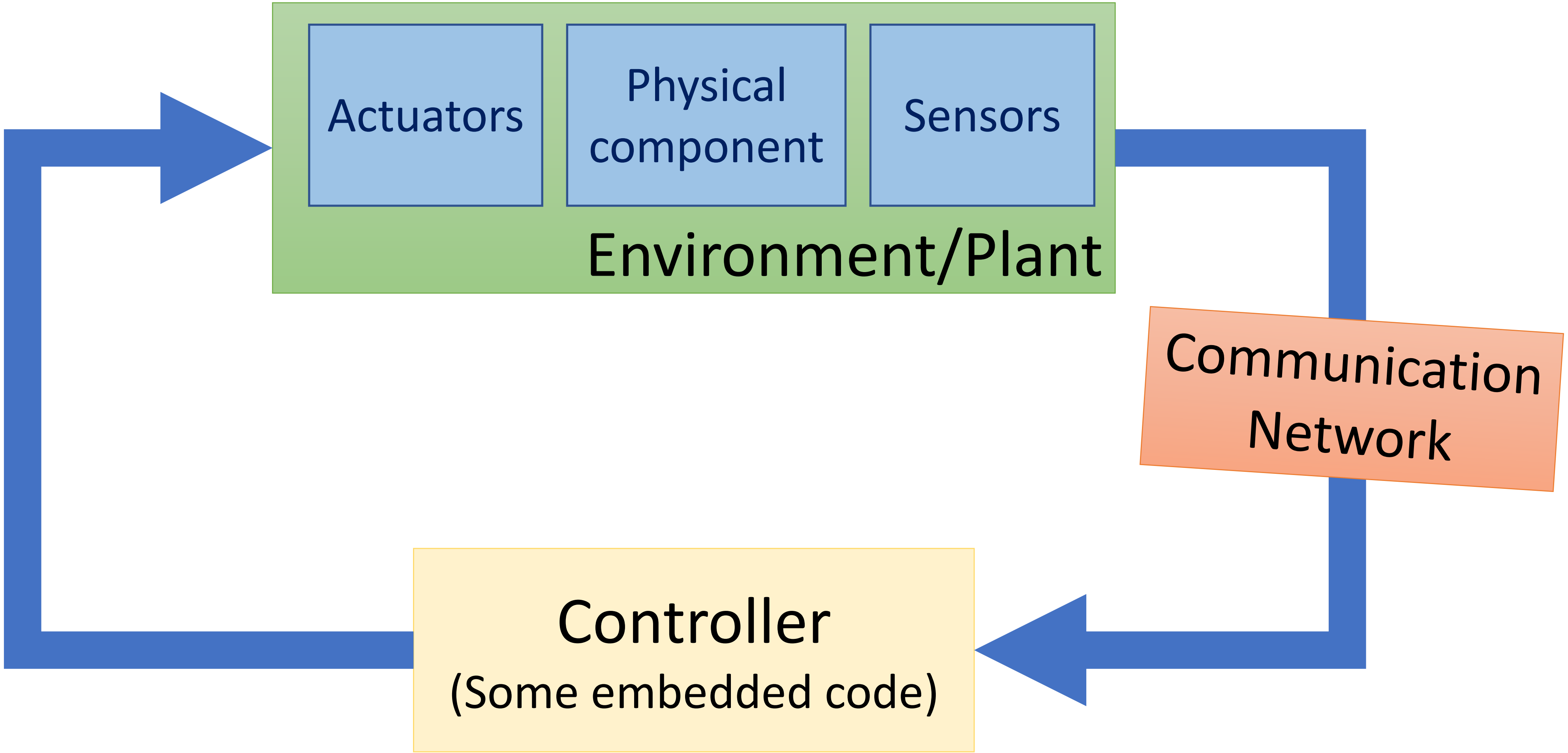


Cyber part
(Decision Maker)

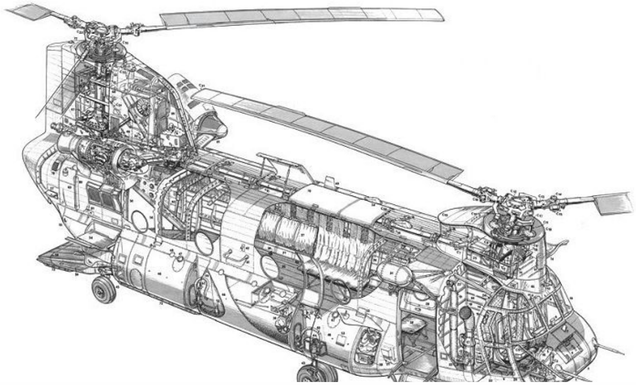
Physical part
(Controlled system)

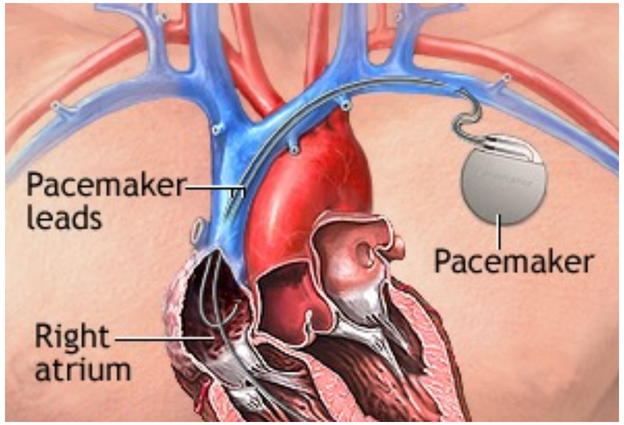
Networked
Internet of Things

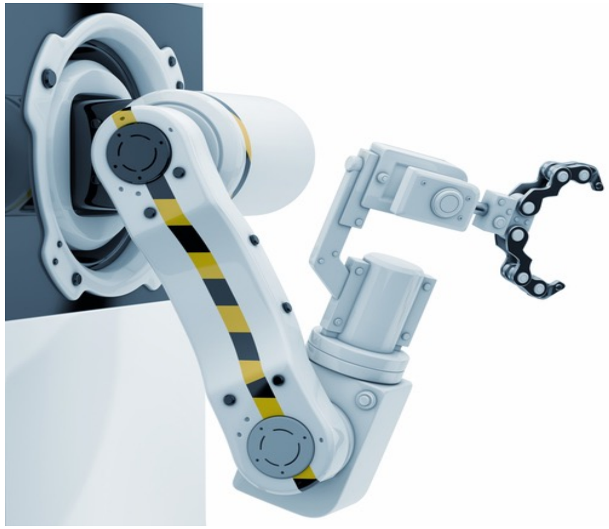
Our view of a CPS



Examples

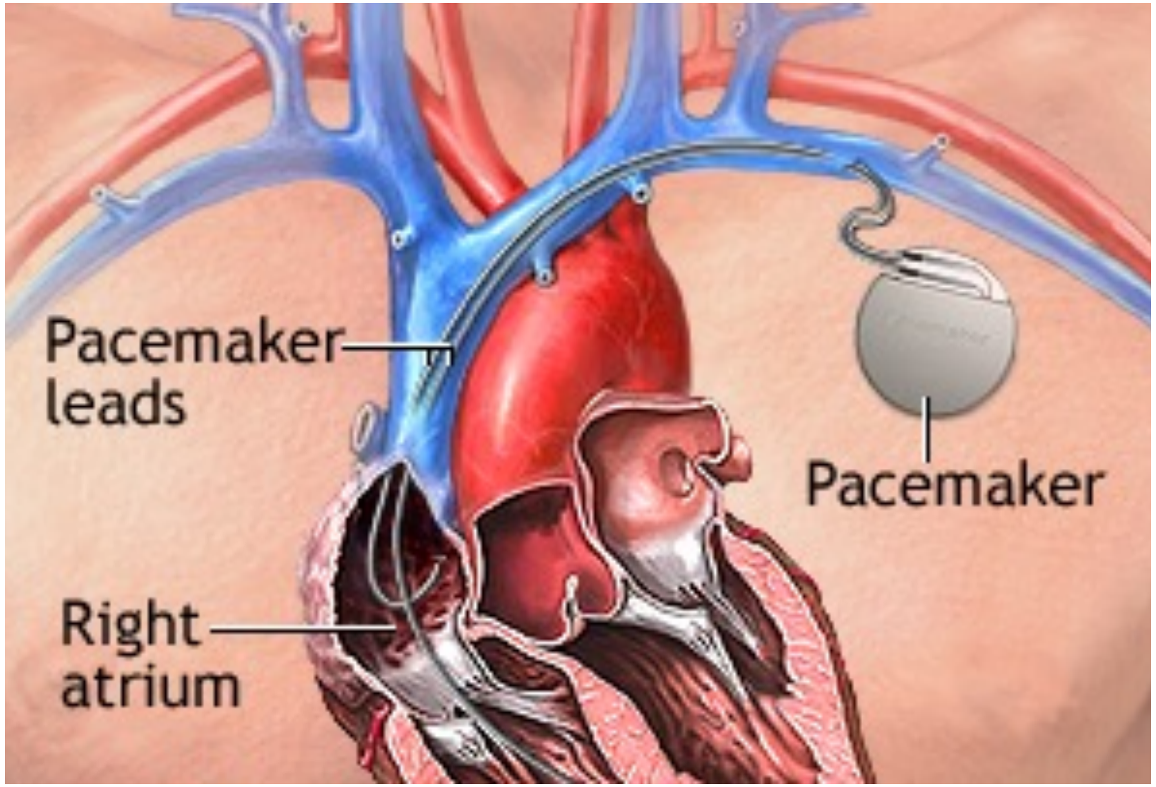


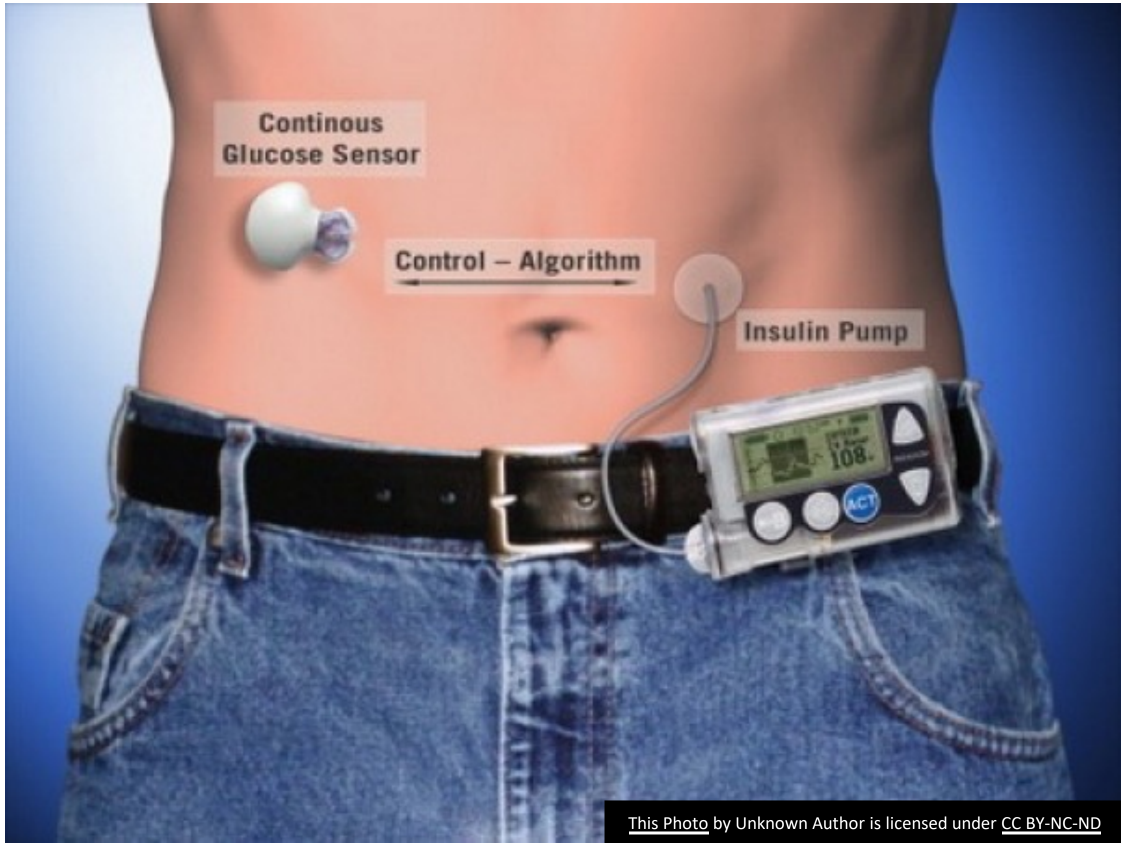




[All images from Google image search]

Medical Device

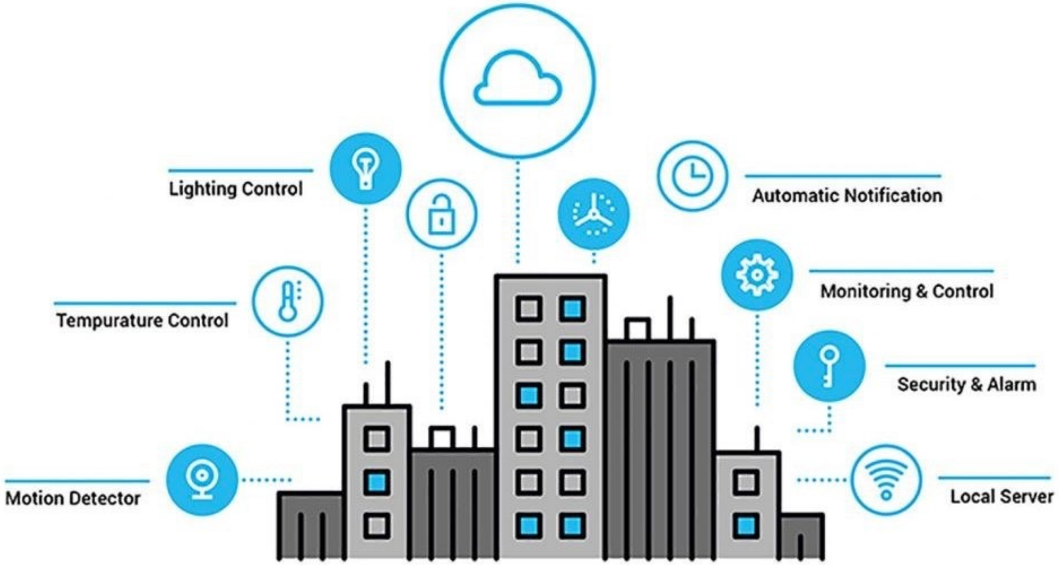




Transportation CPS

Everything that moves will become autonomous

Energy


Lighting Control
Automatic Notification
Tempurature Control
Monitoring & Control
Security & Alarm
Motion Detector
Local Server

© Siemens

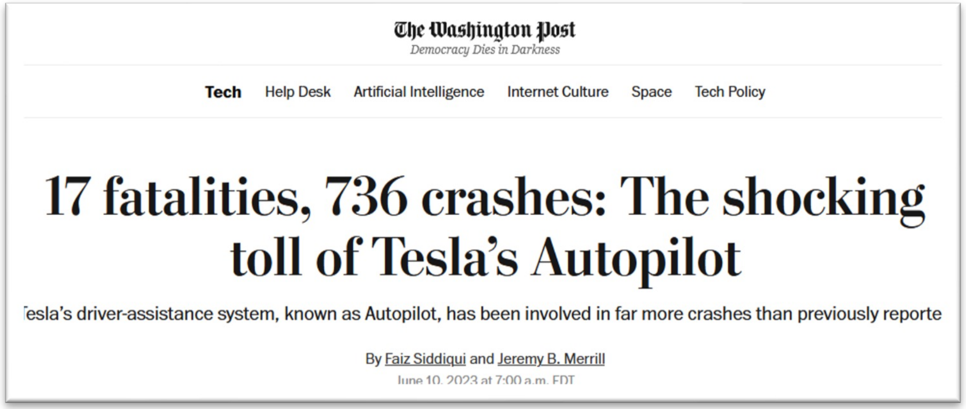
And many other applications…

- Robotics
- Critical Infrastructures
- Industrial Control
- Manufactering
- Agricolture

Autonomous CPS

- Autonomous: without the need for human intervention or control
- Autonomous CPS = CPS with no human operator!
- Semi-autonomous: CPS with autonomy under specific conditions but requiring a human operator otherwise.
- Today, several CPS examples are semi-autonomous, and getting to fully autonomous

Are we safe ?

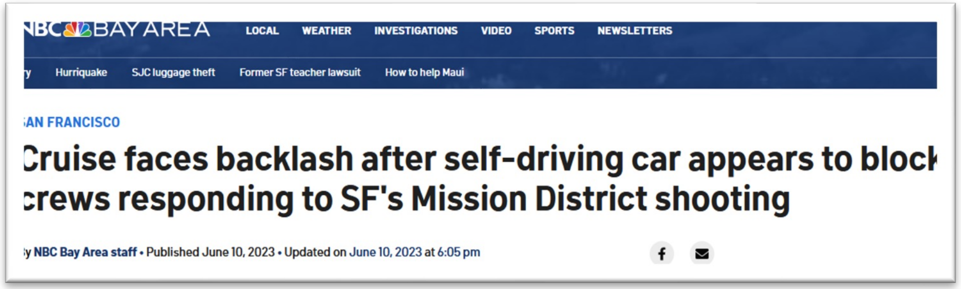


17 fatalities, 736 crashes: The shocking toll of Tesla's Autopilot

esla's driver-assistance system, known as Autopilot, has been involved in far more crashes than previously reporte

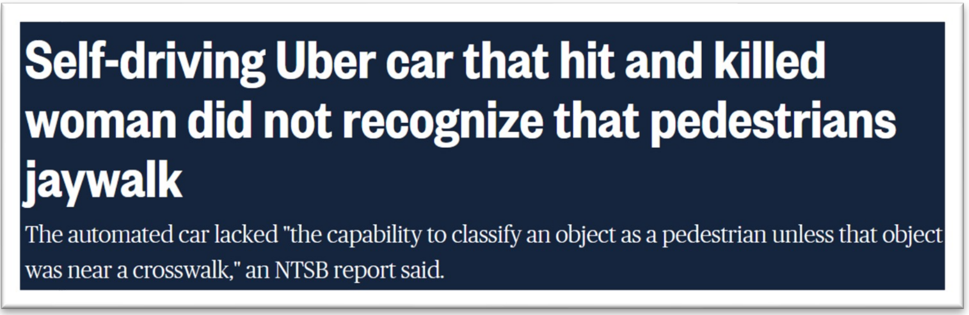
By Faiz Siddiqui and Jeremy B. Merrill

June 10, 2023 at 7:00 a.m. EDT



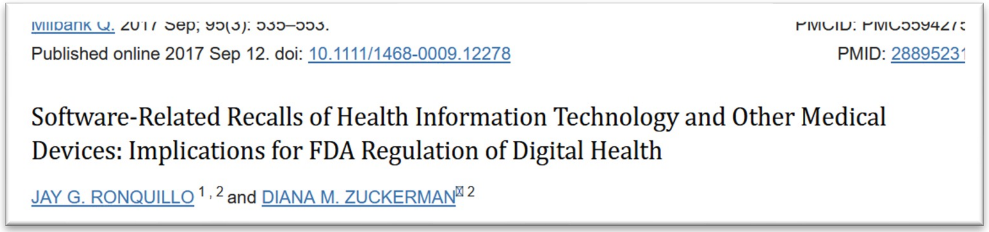
Cruise faces backlash after self-driving car appears to block crews responding to SF's Mission District shooting

y NBC Bay Area staff • Published June 10, 2023 • Updated on June 10, 2023 at 6:05 pm



Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk

The automated car lacked "the capability to classify an object as a pedestrian unless that object was near a crosswalk," an NTSB report said.

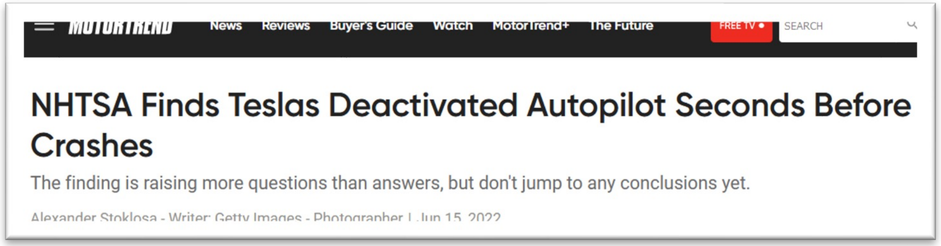


Milbank Q. 2017 Sep; 95(3): 535–553.
Published online 2017 Sep 12. doi: 10.1111/1468-0009.12278

PMCID: PMC559427
PMID: 2889523

Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health

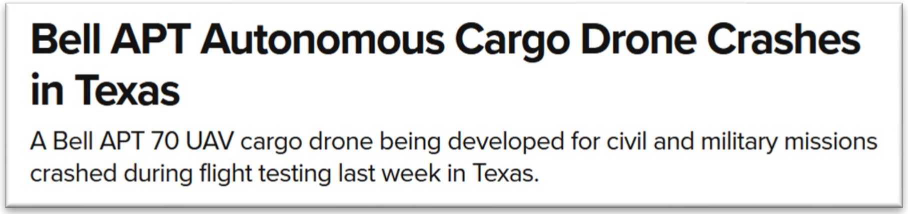
JAY G. RONQUILLO[1, 2] and DIANA M. ZUCKERMAN[2]



NHTSA Finds Teslas Deactivated Autopilot Seconds Before Crashes

The finding is raising more questions than answers, but don't jump to any conclusions yet.

Alexander Stoklosa - Writer; Getty Images - Photographer | Jun 15, 2022

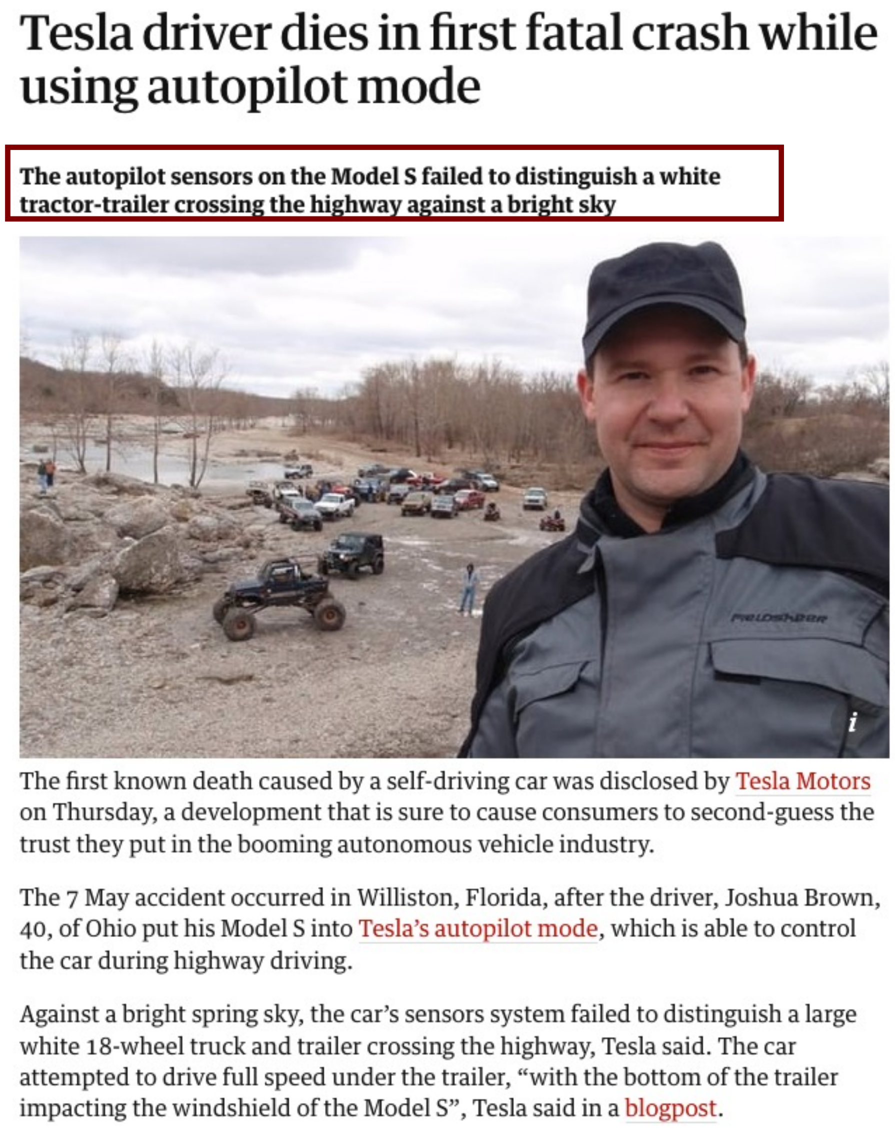


Bell APT Autonomous Cargo Drone Crashes in Texas

A Bell APT 70 UAV cargo drone being developed for civil and military missions crashed during flight testing last week in Texas.

ACPS are safety-critical, and/or mission-critical with huge implications on human health, well-being, economy, etc.

Some tragic accidents



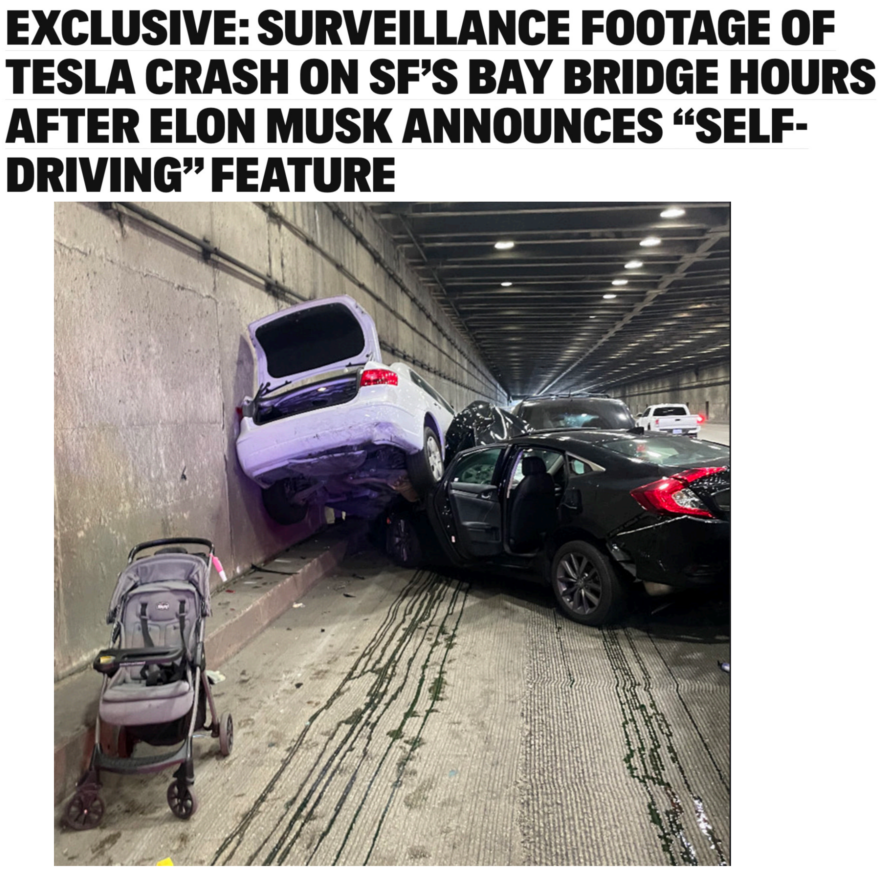
Tesla driver dies in first fatal crash while using autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky

The first known death caused by a self-driving car was disclosed by Tesla Motors on Thursday, a development that is sure to cause consumers to second-guess the trust they put in the booming autonomous vehicle industry.

The 7 May accident occurred in Williston, Florida, after the driver, Joshua Brown, 40, of Ohio put his Model S into Tesla's autopilot mode, which is able to control the car during highway driving.

Against a bright spring sky, the car's sensors system failed to distinguish a large white 18-wheel truck and trailer crossing the highway, Tesla said. The car attempted to drive full speed under the trailer, "with the bottom of the trailer impacting the windshield of the Model S", Tesla said in a blogpost.

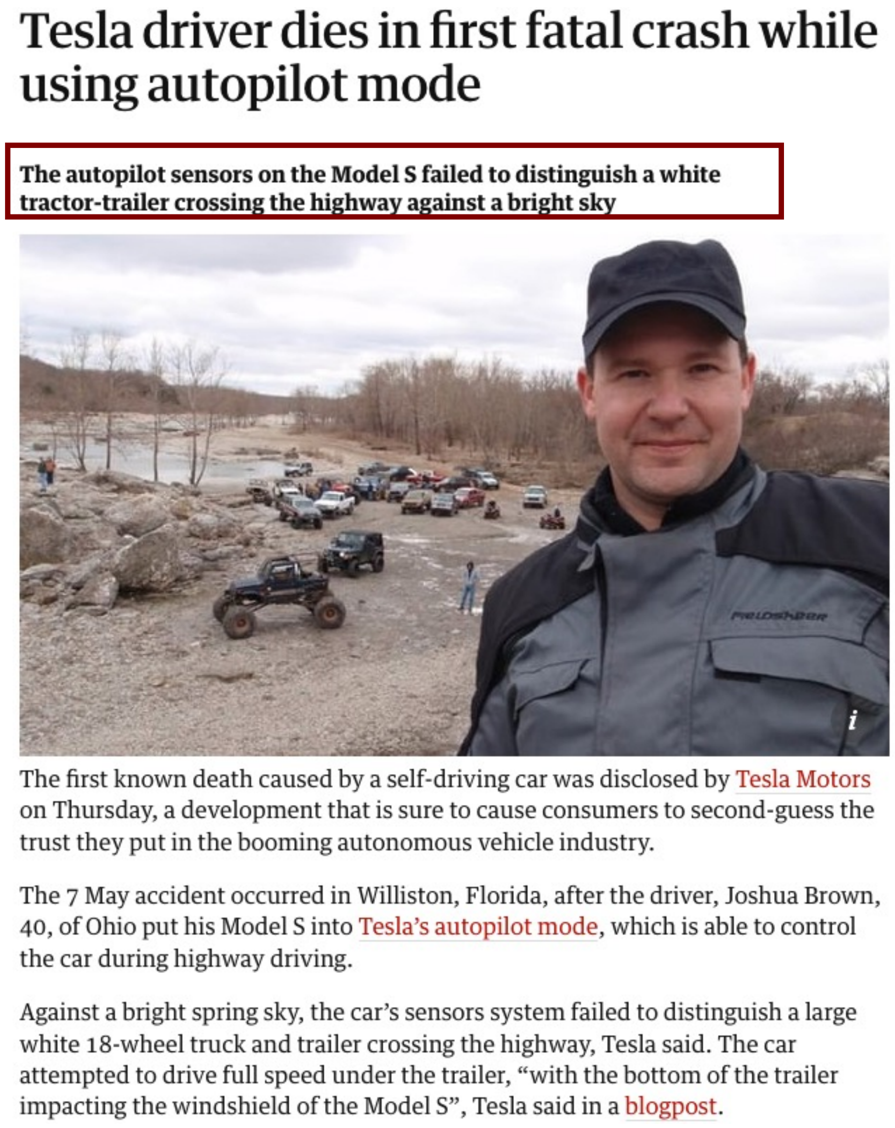


EXCLUSIVE: SURVEILLANCE FOOTAGE OF TESLA CRASH ON SF'S BAY BRIDGE HOURS AFTER ELON MUSK ANNOUNCES "SELF-DRIVING" FEATURE

Highway surveillance footage from November 24 shows a Tesla Model S vehicle changing lanes and then abruptly braking in the far-left lane of the San Francisco Bay Bridge, resulting in an eight-vehicle crash.

https://theintercept.com/2023/01/10/tesla-crash-footage-autopilot/

Some tragic accidents



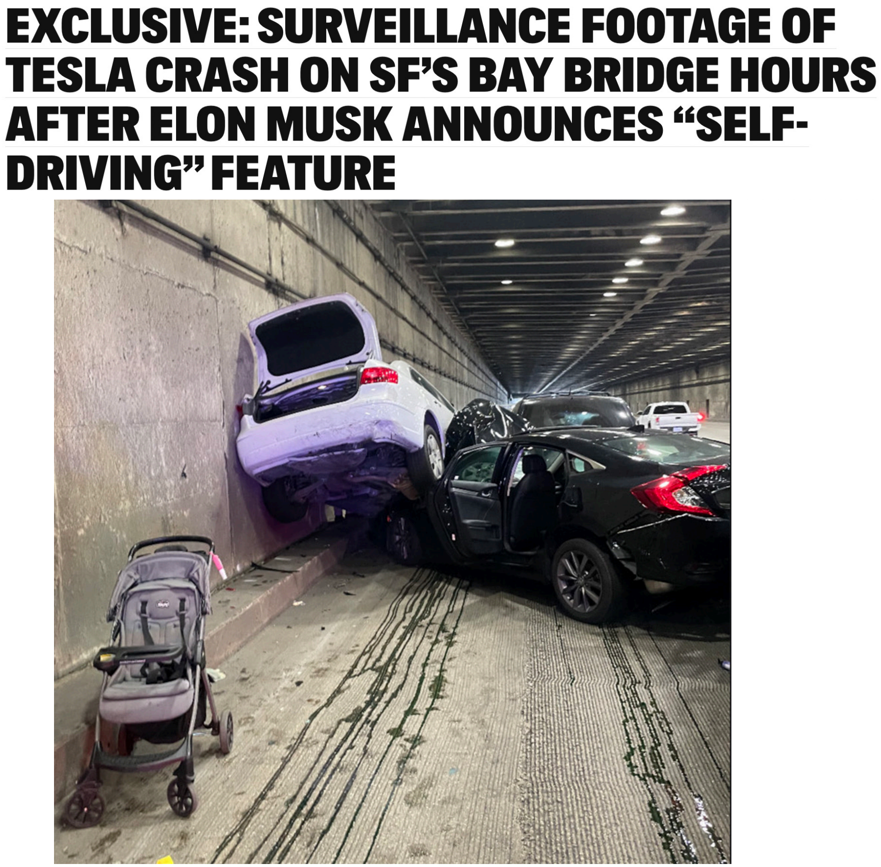
Tesla driver dies in first fatal crash while using autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky

The first known death caused by a self-driving car was disclosed by Tesla Motors on Thursday, a development that is sure to cause consumers to second-guess the trust they put in the booming autonomous vehicle industry.

The 7 May accident occurred in Williston, Florida, after the driver, Joshua Brown, 40, of Ohio put his Model S into Tesla's autopilot mode, which is able to control the car during highway driving.

Against a bright spring sky, the car's sensors system failed to distinguish a large white 18-wheel truck and trailer crossing the highway, Tesla said. The car attempted to drive full speed under the trailer, "with the bottom of the trailer impacting the windshield of the Model S", Tesla said in a blogpost.

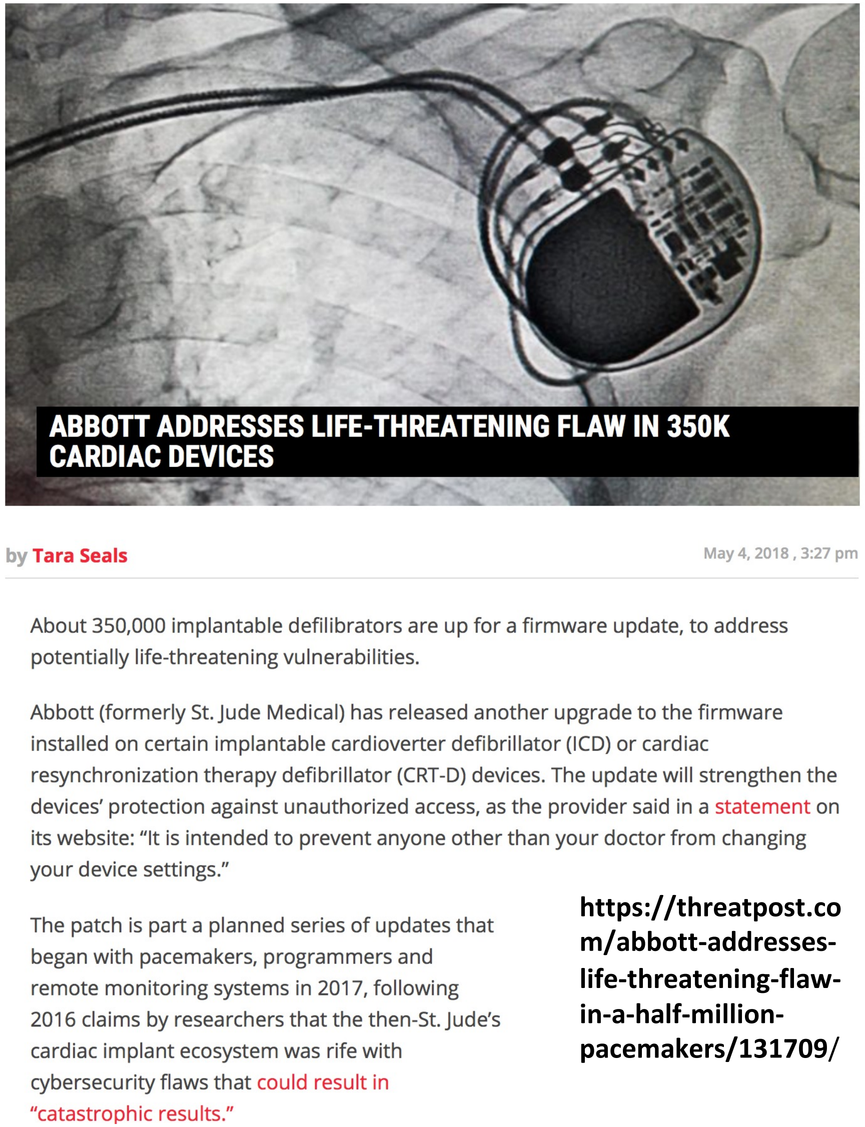


EXCLUSIVE: SURVEILLANCE FOOTAGE OF TESLA CRASH ON SF'S BAY BRIDGE HOURS AFTER ELON MUSK ANNOUNCES "SELF-DRIVING" FEATURE

Musk said that "Full Self-Driving" was an "essential" feature for Tesla to develop, going as far as saying, "It's really the difference between Tesla being worth a lot of money or worth basically zero."

https://theintercept.com/2023/01/10/tesla-crash-footage-autopilot/

Are we safe ?



ABBOTT ADDRESSES LIFE-THREATENING FLAW IN 350K CARDIAC DEVICES

by Tara Seals

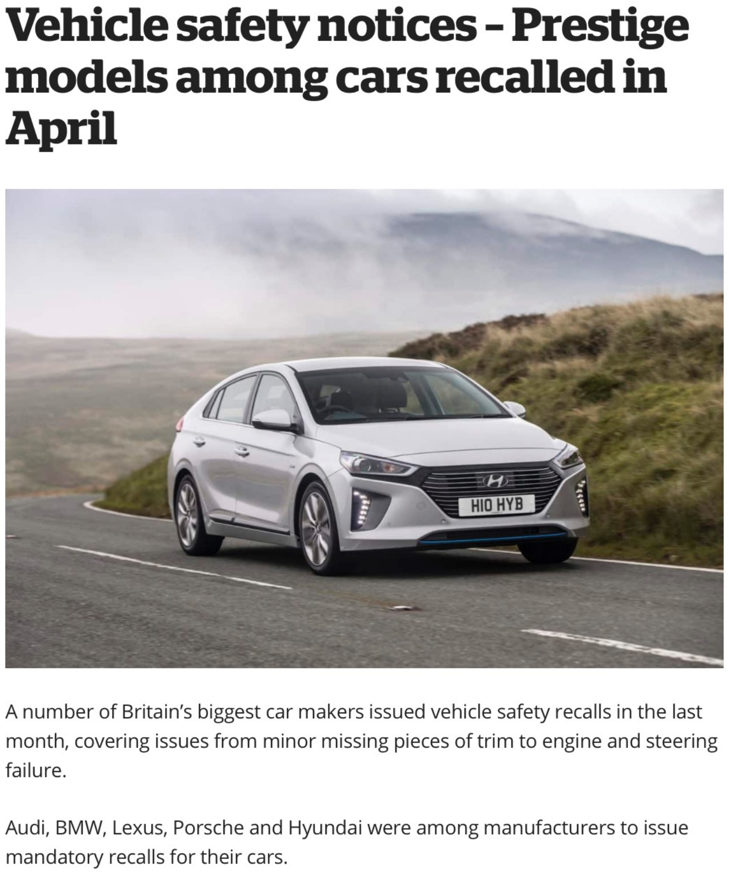
May 4, 2018 , 3:27 pm

About 350,000 implantable defilibrators are up for a firmware update, to address potentially life-threatening vulnerabilities.

Abbott (formerly St. Jude Medical) has released another upgrade to the firmware installed on certain implantable cardioverter defibrillator (ICD) or cardiac resynchronization therapy defibrillator (CRT-D) devices. The update will strengthen the devices' protection against unauthorized access, as the provider said in a statement on its website: "It is intended to prevent anyone other than your doctor from changing your device settings."

The patch is part a planned series of updates that began with pacemakers, programmers and remote monitoring systems in 2017, following 2016 claims by researchers that the then-St. Jude's cardiac implant ecosystem was rife with cybersecurity flaws that could result in "catastrophic results."

https://threatpost.com/abbott-addresses-life-threatening-flaw-in-a-half-million-pacemakers/131709/



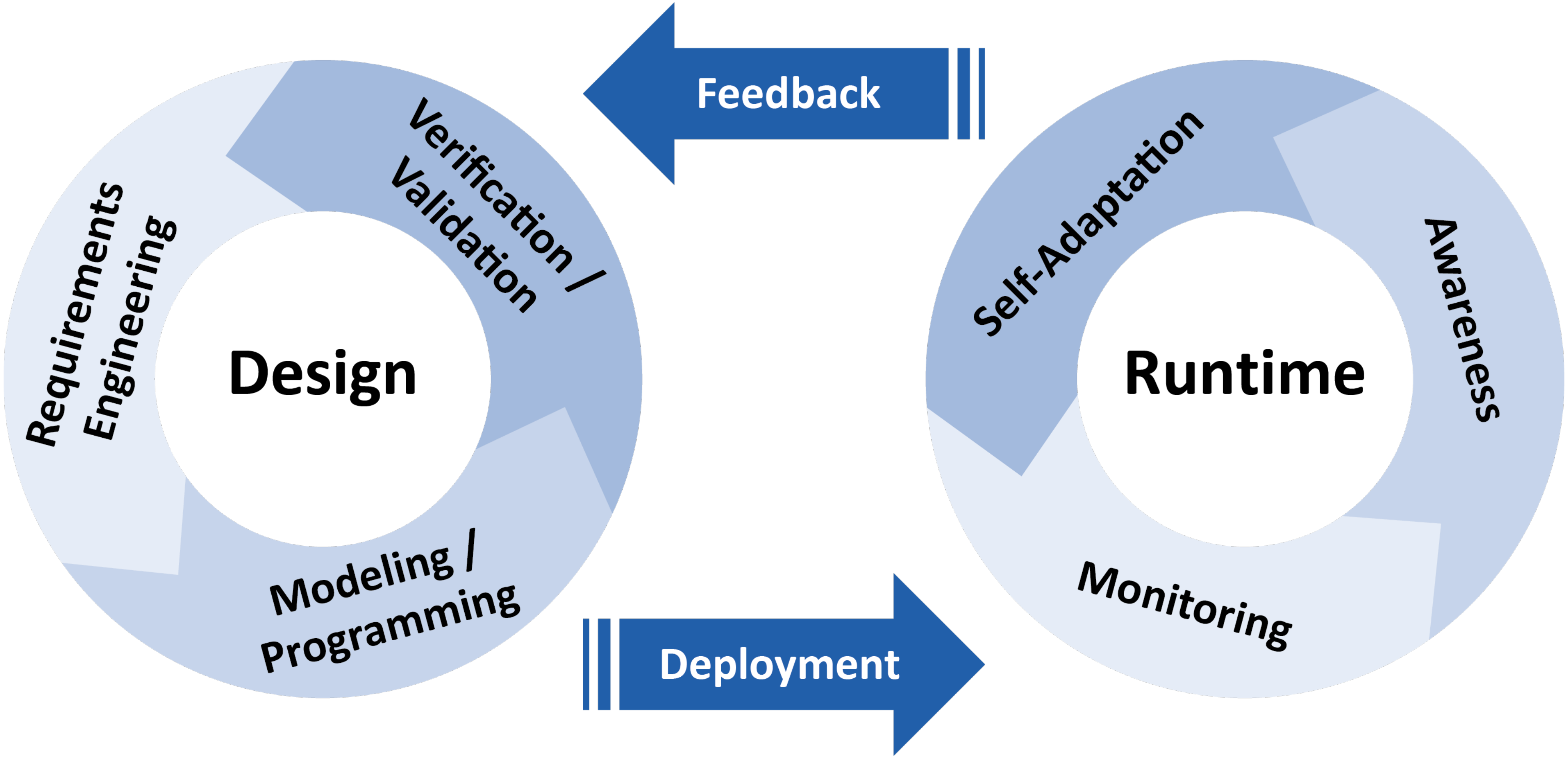
Vehicle safety notices – Prestige models among cars recalled in April

A number of Britain's biggest car makers issued vehicle safety recalls in the last month, covering issues from minor missing pieces of trim to engine and steering failure.

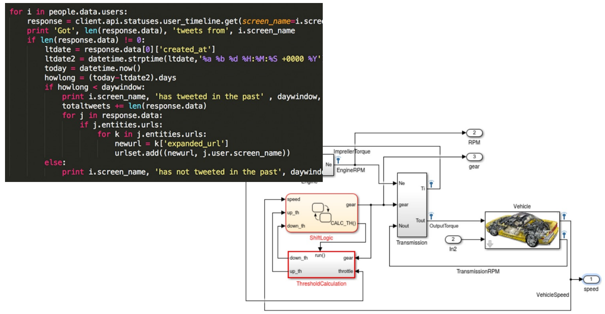
Audi, BMW, Lexus, Porsche and Hyundai were among manufacturers to issue mandatory recalls for their cars.

https://inews.co.uk/essentials/lifestyle/cars/car-news/vehicle-safety-recalls-notices-prestige-cars-recalled-april/

Rigorous Engineering of CPS



Model-Based Design



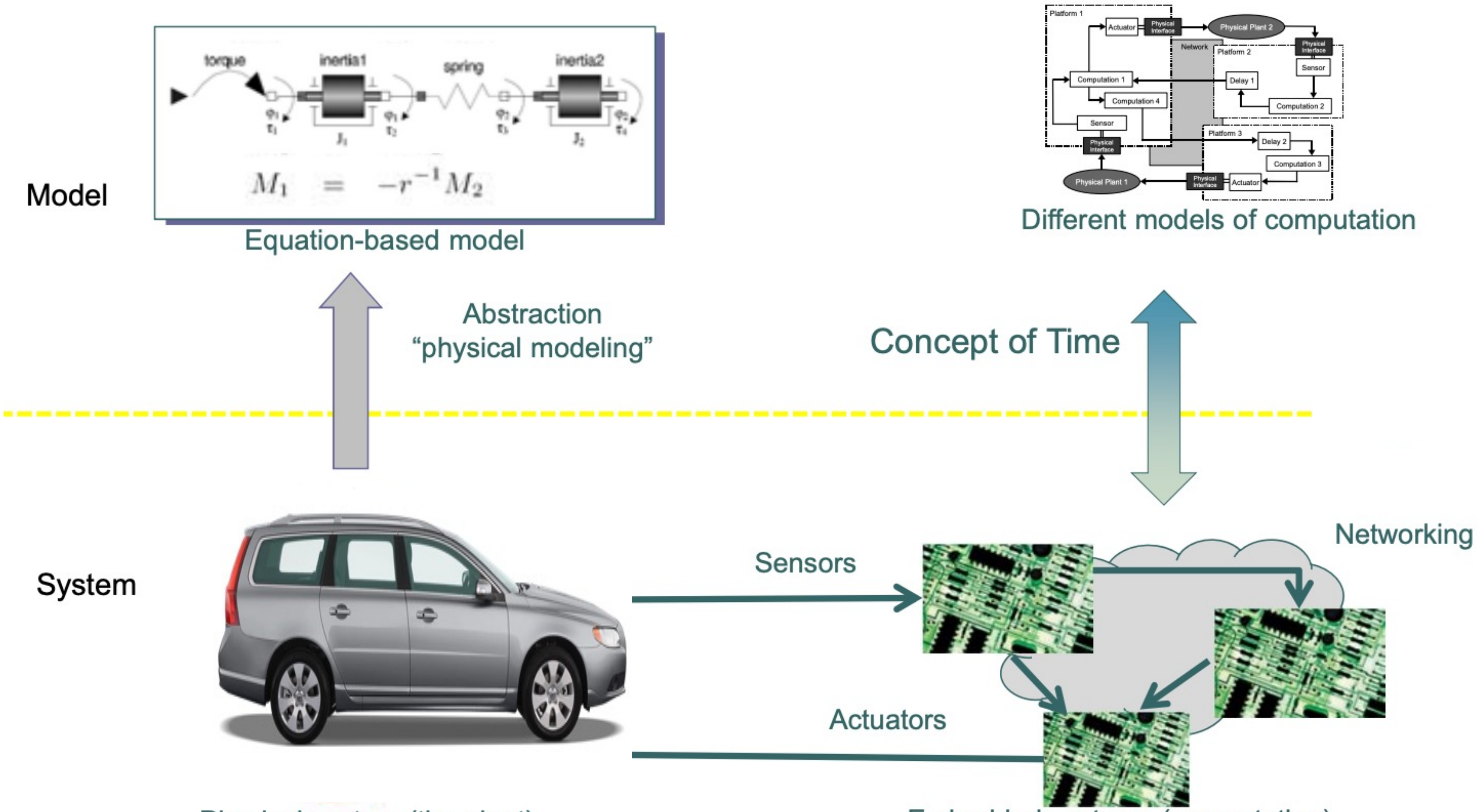
```
for i in people.data.users:
    response = client.api.statuses.user_timeline.get(screen_name=i.scre
    print 'Got', len(response.data), 'tweets from', i.screen_name
    if len(response.data) != 0:
        ltdate = response.data[0]['created_at']
        ltdate2 = datetime.strptime(ltdate,'%a %b %d %H:%M:%S +0000 %Y'
        today = datetime.now()
        howlong = (today-ltdate2).days
        if howlong < daywindow:
            print i.screen_name, 'has tweeted in the past' , daywindow,
            totaltweets += len(response.data)
            for j in response.data:
                if j.entities.urls:
                    for k in j.entities.urls:
                        newurl = k['expanded_url']
                        urlset.add((newurl, j.user.screen_name))
        else:
            print i.screen_name, 'has not tweeted in the past', daywind
```

Requirement Definition

Design/Implementation

Verification

Model-based Design Approach



Model

$$M_1 = -r^{-1} M_2$$

Equation-based model

Different models of computation

Abstraction
"physical modeling"

Concept of Time

System

Sensors

Networking

Actuators

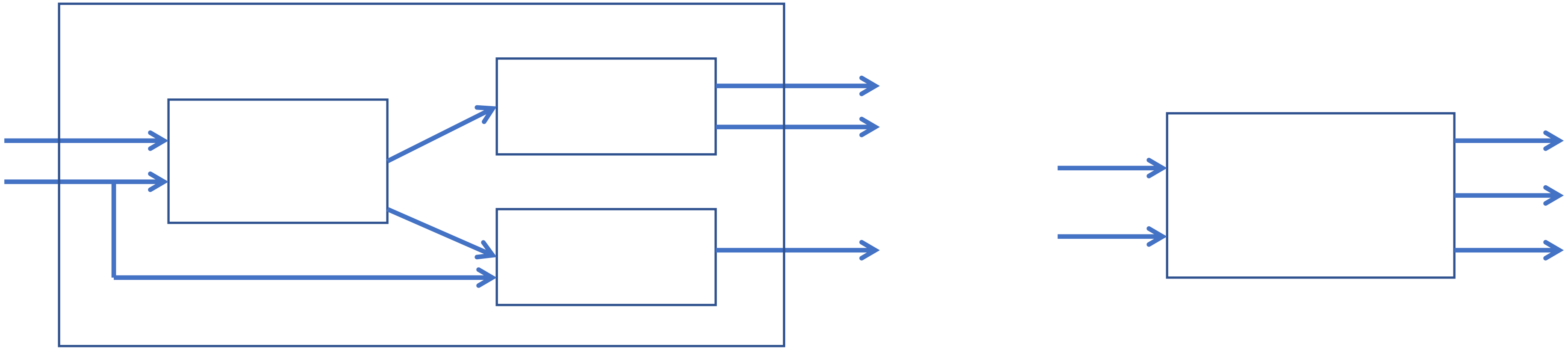
Physical system (the plant)

Embedded systems (computation)

Courtesy: D. Broman

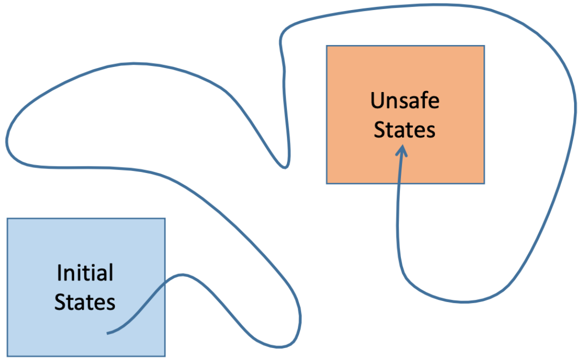
Model-based Design Approach

- MBD when used for designing embedded software[1] has 4 main steps
  1. Model the physical components/environment (also known as a plant model)
  2. Analyze the plant, and synthesize/design the control-software at a high-level
  3. Co-Simulate the plant and control-software
  4. Automatically generate code from the control-software model for deployment
- MBD languages are often visual and block-diagram based, e.g. Simulink

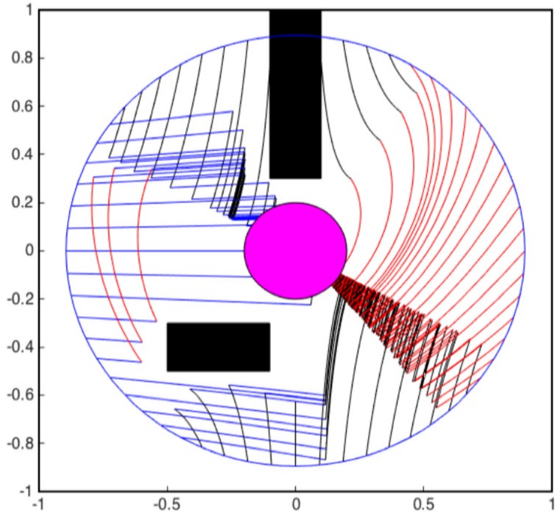


[1] Nicolescu, Gabriela; Mosterman, Pieter J., eds. (2010). Model-Based Design for Embedded Systems. Computational Analysis, Synthesis, and Design of Dynamic Systems. 1. Boca Raton: CRC Press.

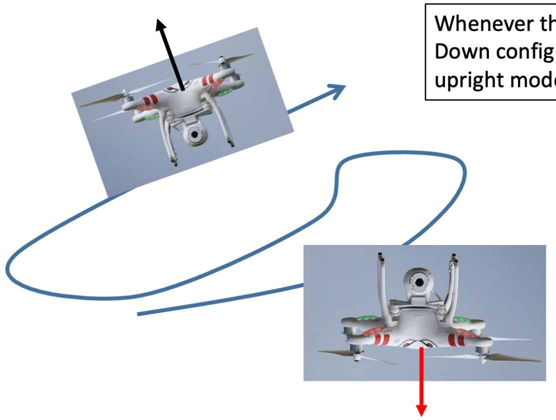
Reachability



Stability



Real-Time Temporal Properties



Whenever the UAV reaches an Upside-Down configuration, it must reach an upright mode within 2 seconds.

Formal Reasoning

Formal Methods

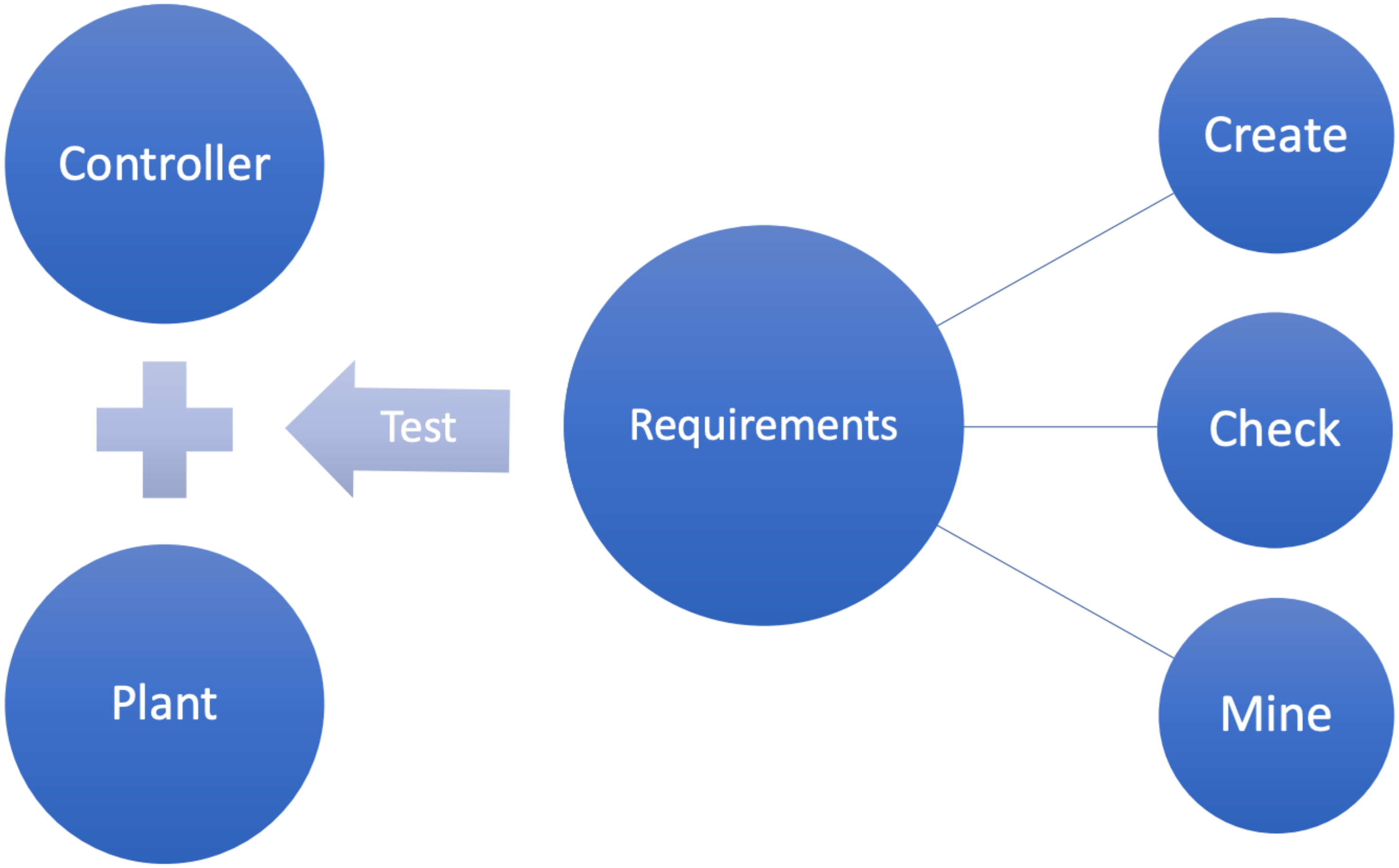
Mathematical, Algorithmic techniques for modeling, design, analysis

– **Specification**: WHAT the system must/must not do

– **Verification**: WHY it meets the spec (or not)

– **Synthesis**: HOW it meets the spec (correct-by-construction design)

Requirement-Driven Design



Requirements formally capture what it means for a system to operate correctly in its operating environment

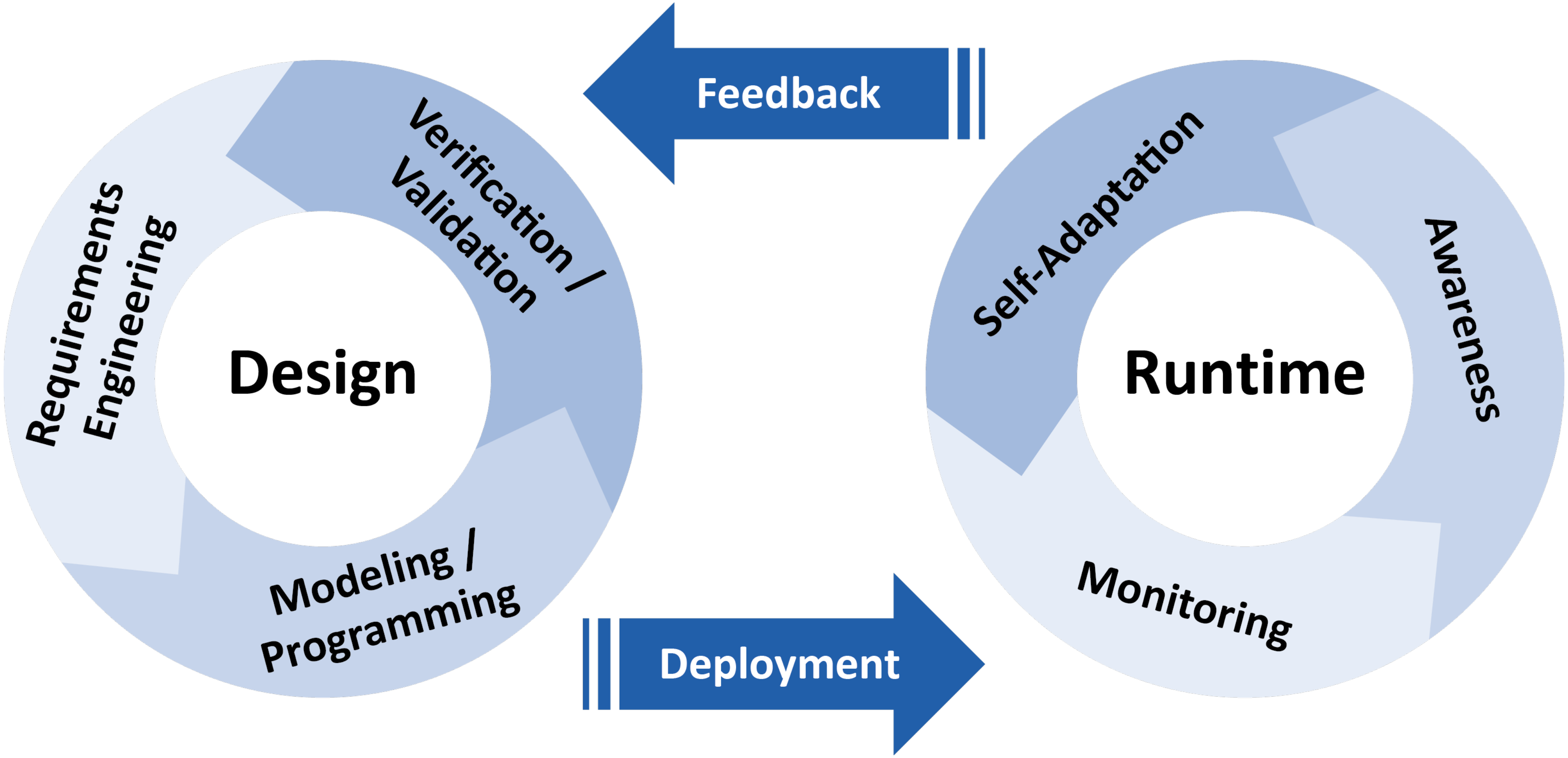
Requirement-Driven Design

Exhaustive verification of CPS is increasingly intractable:

- Openness, environmental change
- Uncertainty, spatial distribution
- Emergent behaviors resulting from the local interactions are not predictable by the analysis of system's individual parts
- Classic state-space explosion problem

How to ensure safety-critical requirements in CPS ?

Rigorous Engineering of CPS



Course Overview

1. Intro to CPS and application domains with example (e.g. Medical CPS, energy CPS, transportation CPS)

2. **Modeling formalism**: ODE systems, Synchronous & Asynchronous Models, Timed Automata, hybrid and switching systems, Basics of Control

3. **Safety:** temporal logic and automata, Monitoring Test Generation, Falsification

4. **Ingredients of Autonomy** for CPS: planning, decision-making, reinforcement learning

Course Objectives

- Gain familiarity with CPS topics

  Challenge Problems/Case studies

- "Model-Based" Software Development Paradigm for CPS

  Developing models for physical components + software (+ communication)

- Writing checkable requirements and tests

Grading

Project (teams of 1-2) with a practice development of a CPS application, verification of formal requirements and falsification or test generation experiments

You can use:

- Matlab/Simulink (simulation) or
- Python or Java if that is the preferred language (it will require additional work for handling requirements but we can help you!) or
- Hypro (Toolbox for the Reachability Analysis of Hybrid Systems)
- Open to other software solution

Report of the Project (no more than 5 pages)

Oral exam with presentation of the Project + general questions on the topics of the course

Example Projects

1. Vehicle model and controller to automatically change lanes
2. Explore multi-vehicle simulators for collaborative merging, autonomous intersection control
3. Pedestrian/bicycle detection and avoidance
4. Traffic simulator for vehicle platooning
5. Create a model of the human heart and design a pacemaker
6. Create a blood-glucose dynamics model and design an automatic insulin infusion pump
7. Train a ground robot that uses LIDAR/Cameras and train it using reinforcement learning

Books (they can just help you)

- Principles of Cyber-Physical Systems, Rajeev Alur, MIT Press, 2015
  https://www.biblio.units.it/SebinaOpac/resource/principles-of-cyberphysical-systems/TSA3289844?tabDoc=tabloceb

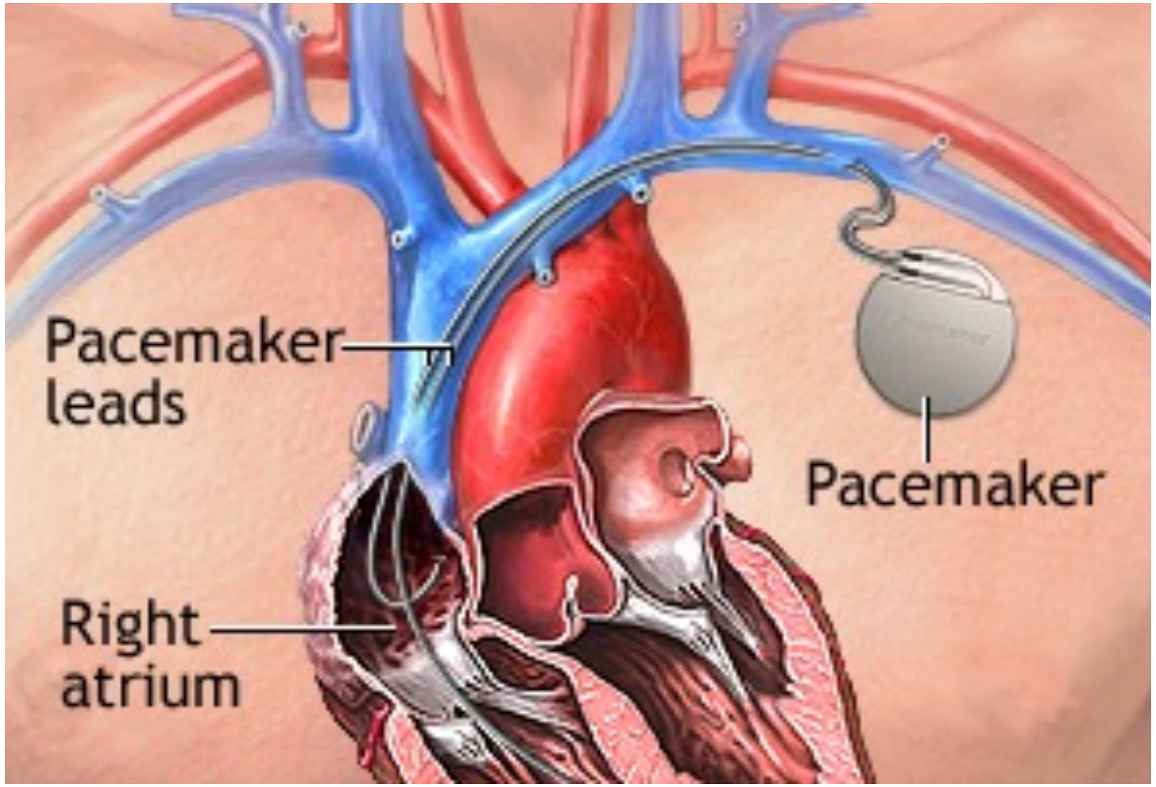
- Introduction to Embedded Systems: A CPS approach
  Free at: https://ptolemy.berkeley.edu/books/leeseshia/
  https://www.biblio.units.it/SebinaOpac/resource/introduction-to-embedded-systems-a-cyberphysical-systems-approach/TSA3289896?tabDoc=tabloceb

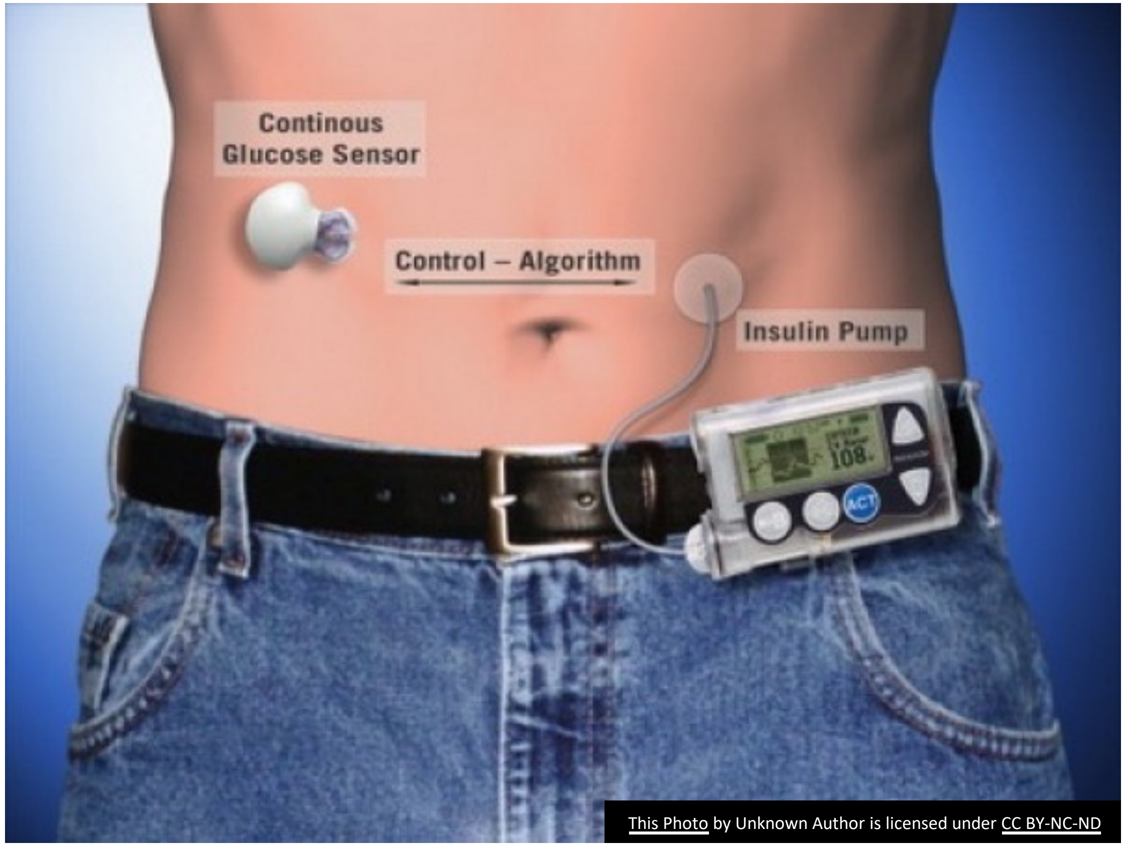
- Principle of Model Checking, Baier, Katoen, MIT Press, 2008

- Reinforcement Learning, An Introduction, RS Sutton, AG Barton, Cambridge, 2011

Questions?

Medical Device

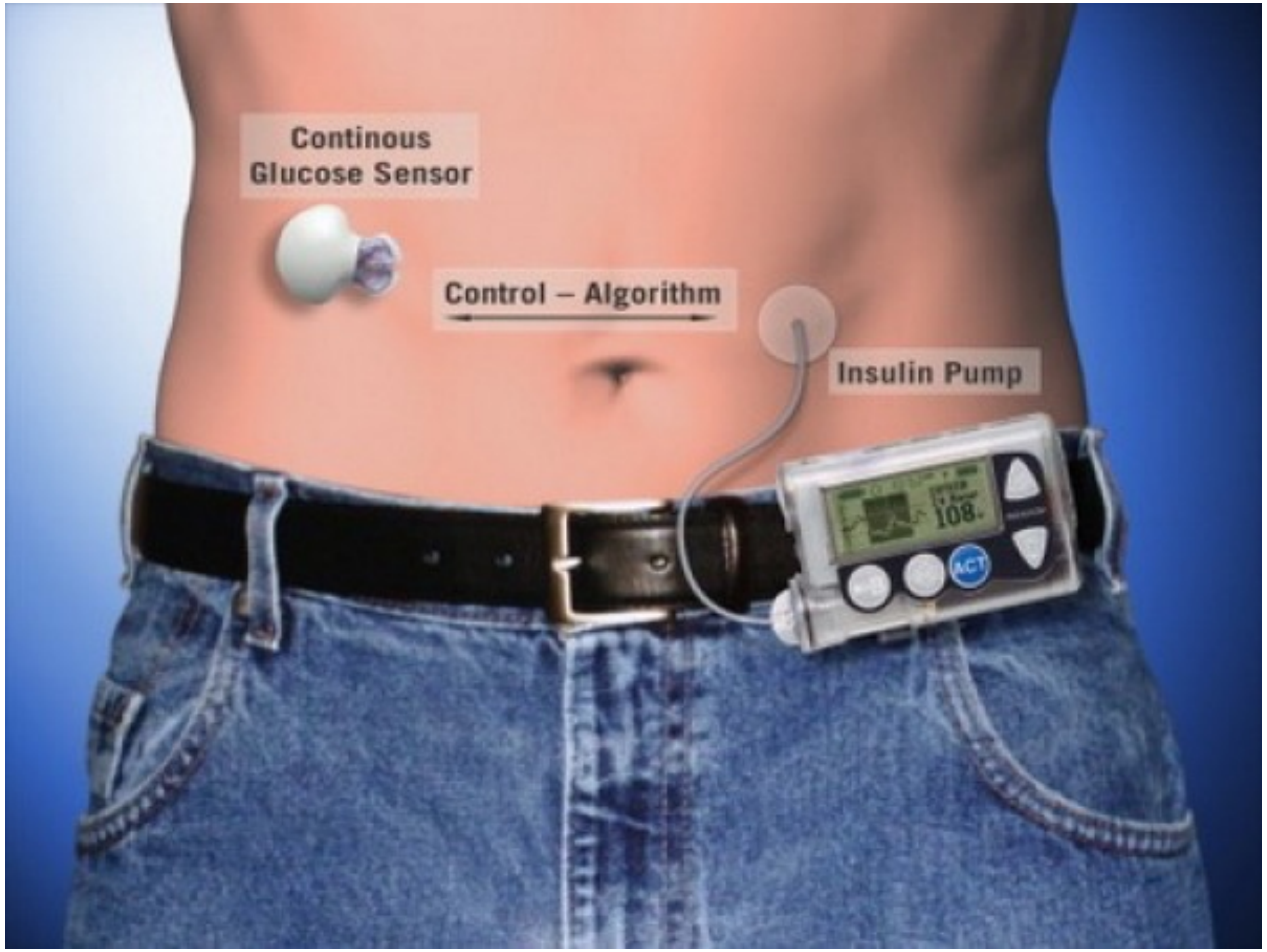




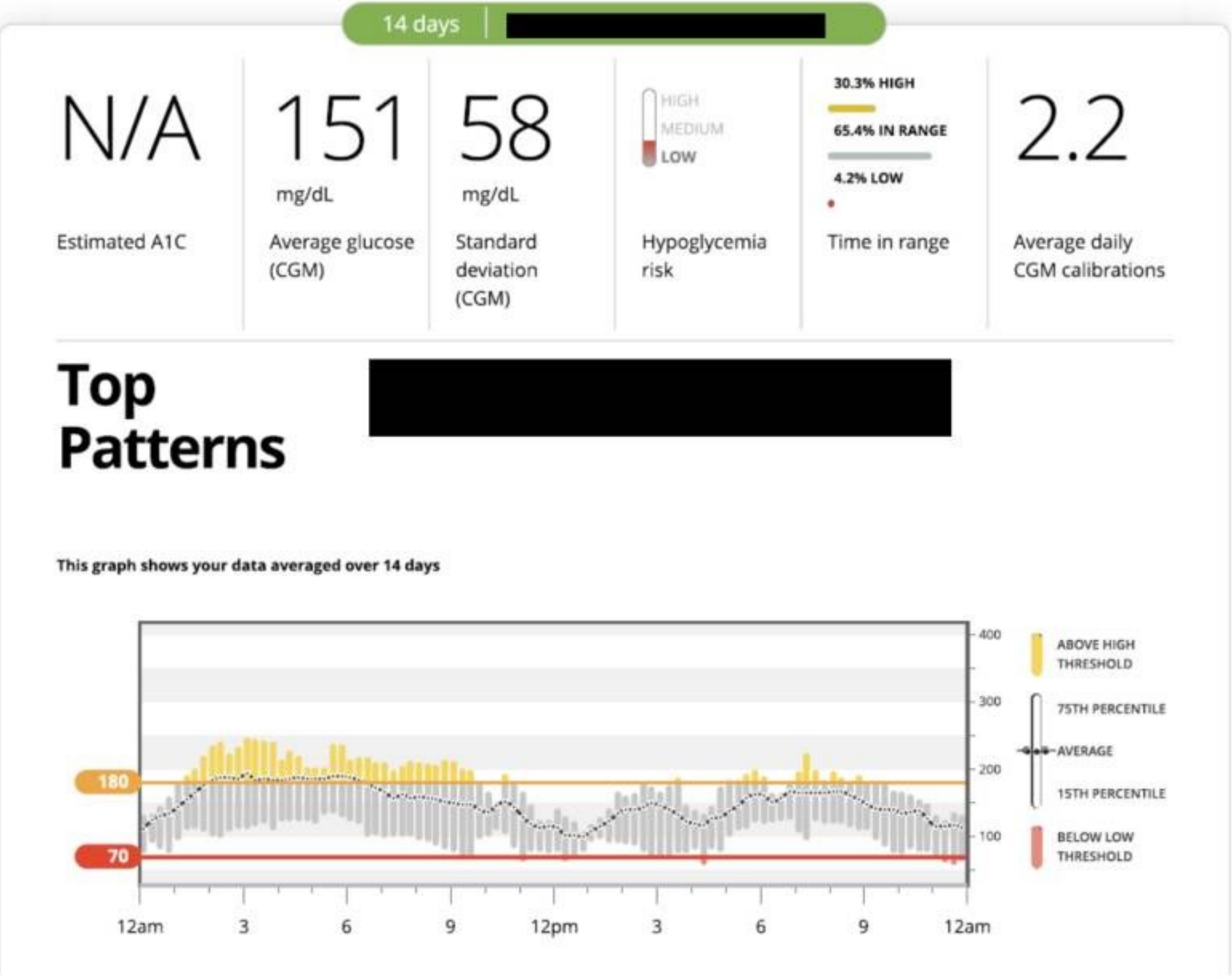
Artificial Pancreas

Type 1 diabetes occurs when the pancreas produces little or none of the insulin needed to regulate blood glucose

They rely on external administration of insulin to manage their blood glucose levels.



Continuous Glucose Monitoring



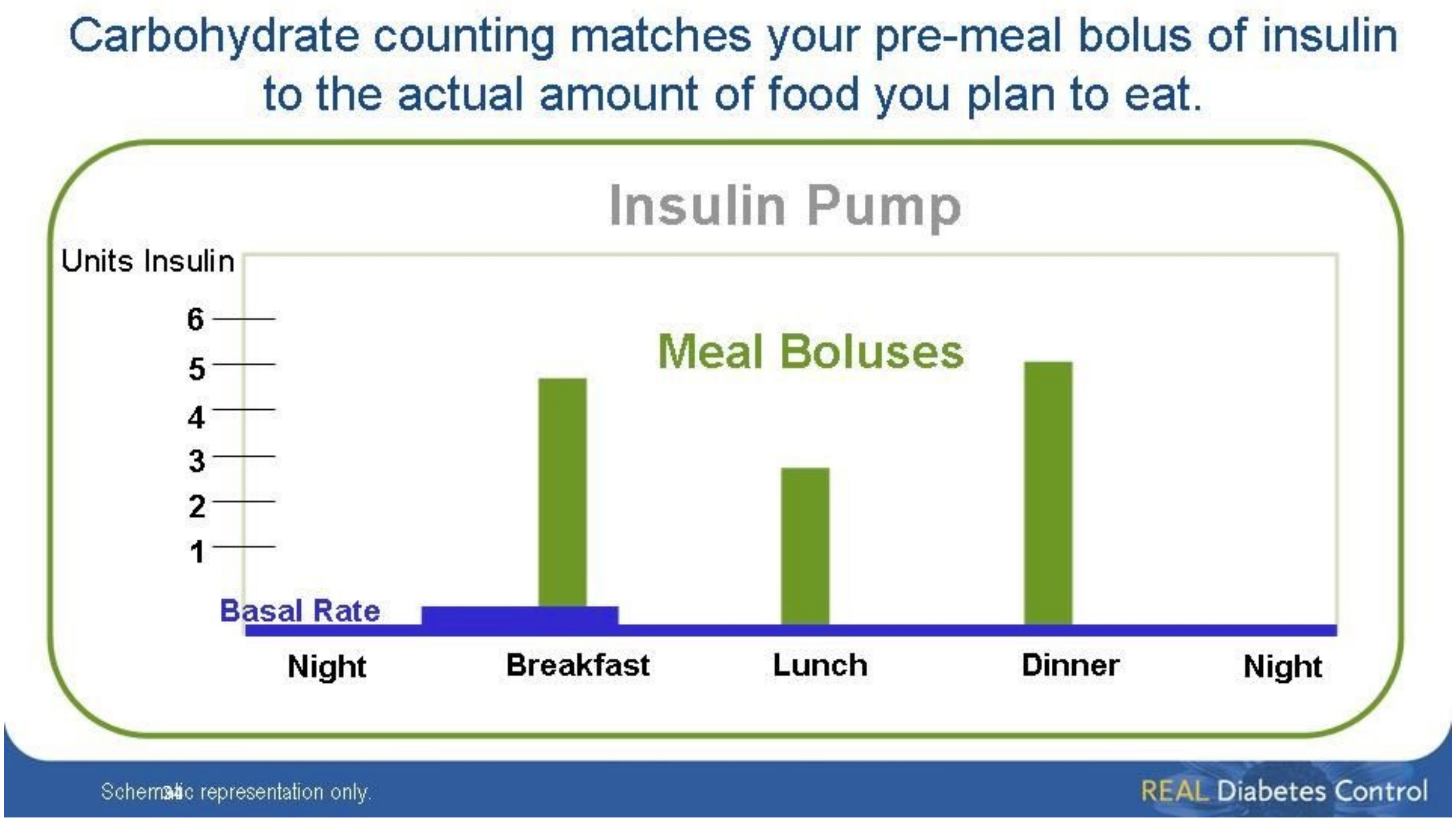
14 days | [redacted]

N/A	151 mg/dL	58 mg/dL	HIGH MEDIUM LOW	30.3% HIGH 65.4% IN RANGE 4.2% LOW	2.2
Estimated A1C	Average glucose (CGM)	Standard deviation (CGM)	Hypoglycemia risk	Time in range	Average daily CGM calibrations

Top Patterns [redacted]

This graph shows your data averaged over 14 days

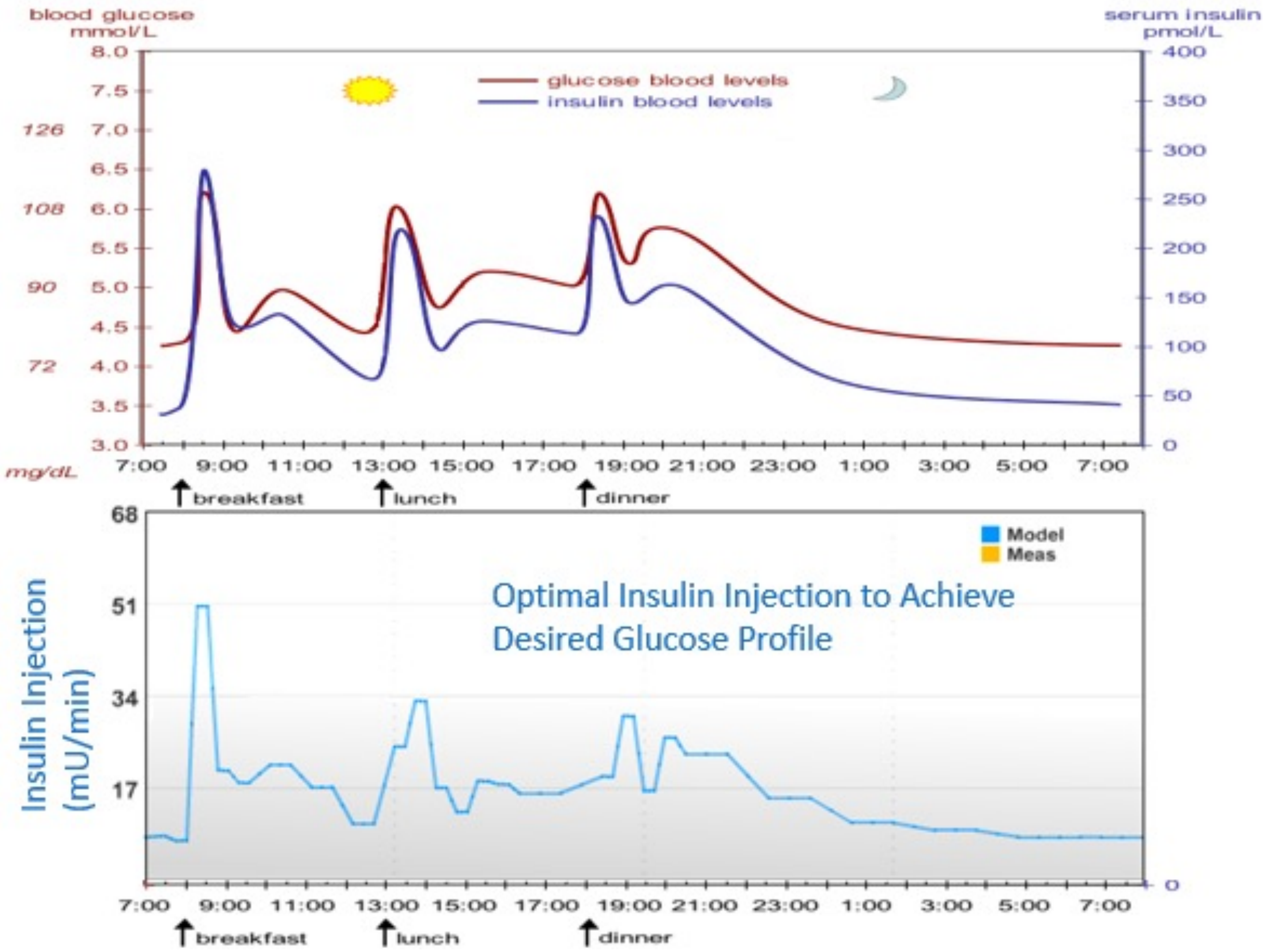
Insulin pumps



Carbohydrate counting matches your pre-meal bolus of insulin to the actual amount of food you plan to eat.

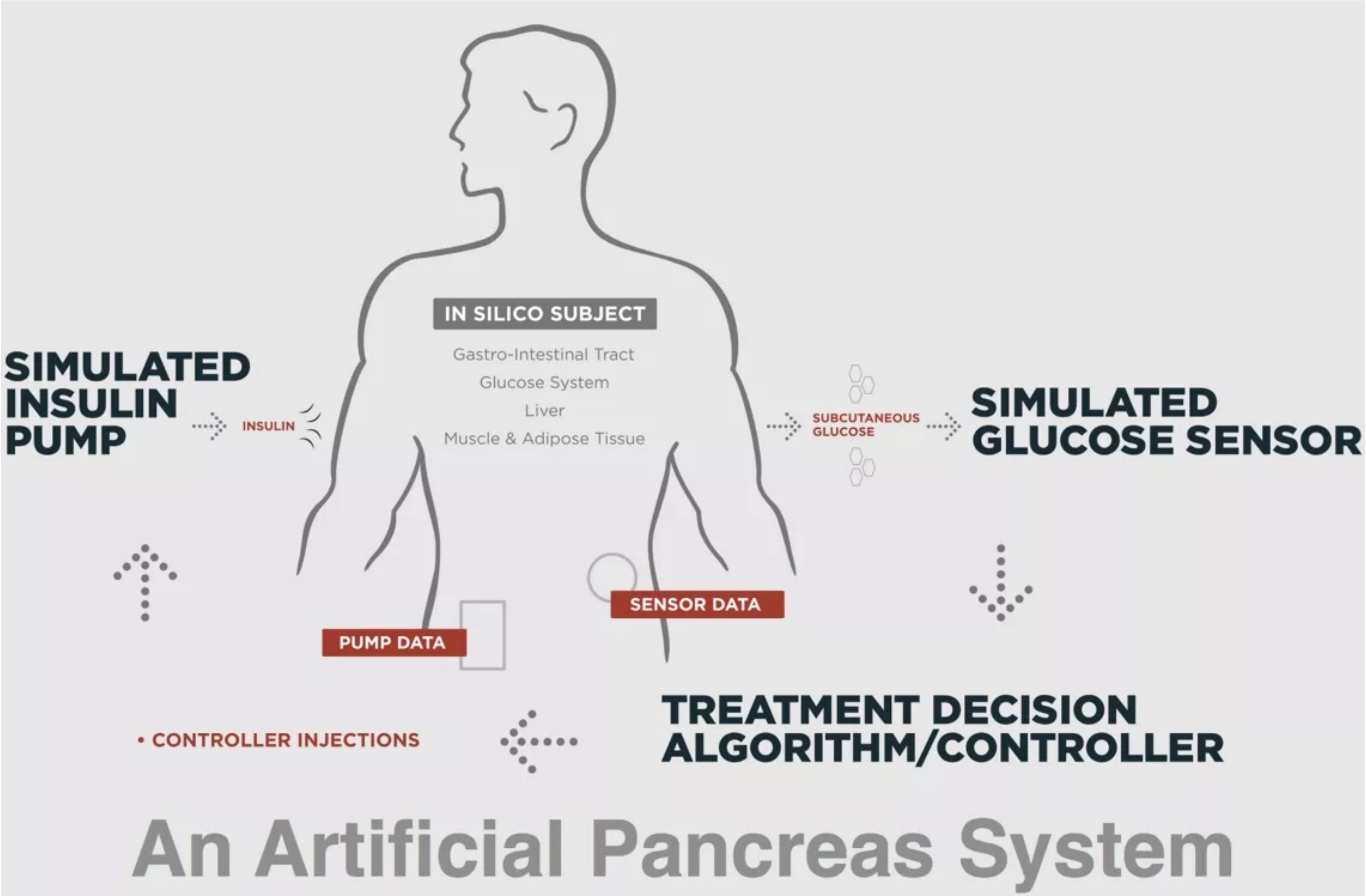
Schematic representation only.

Artificial Pancreas

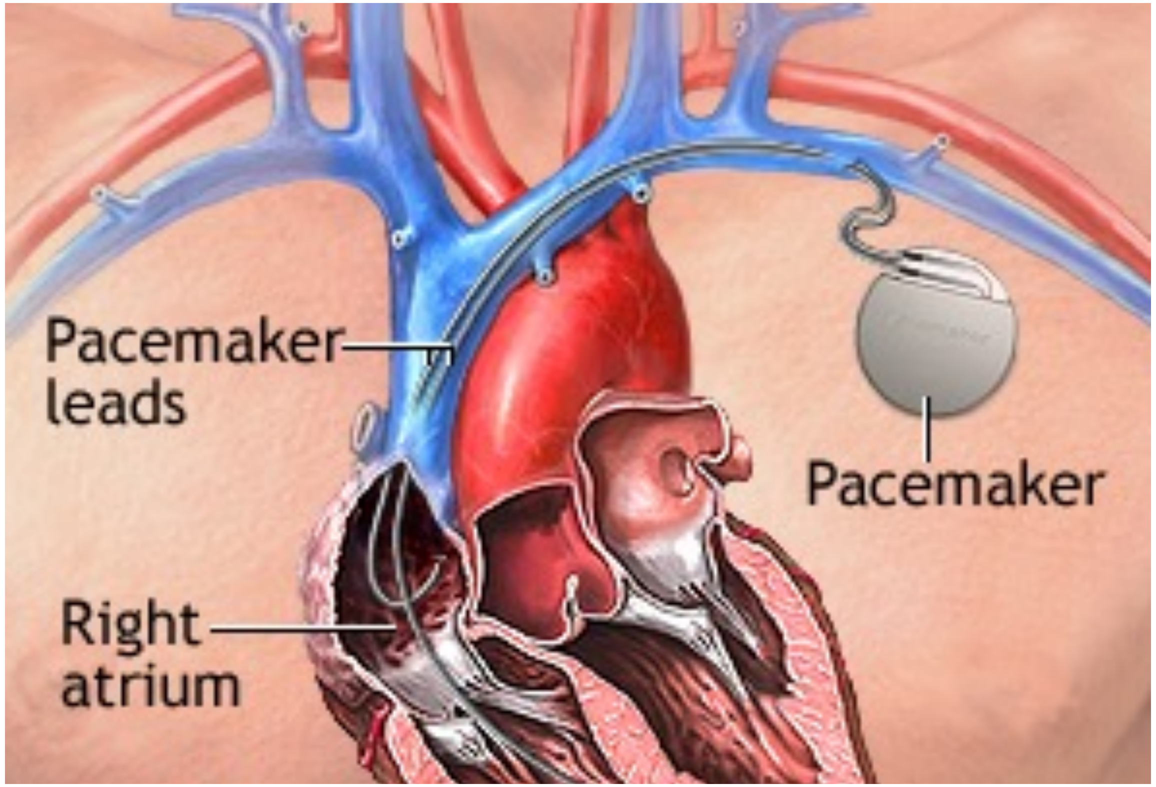


Optimal Insulin Injection to Achieve Desired Glucose Profile

Artificial Pancreas

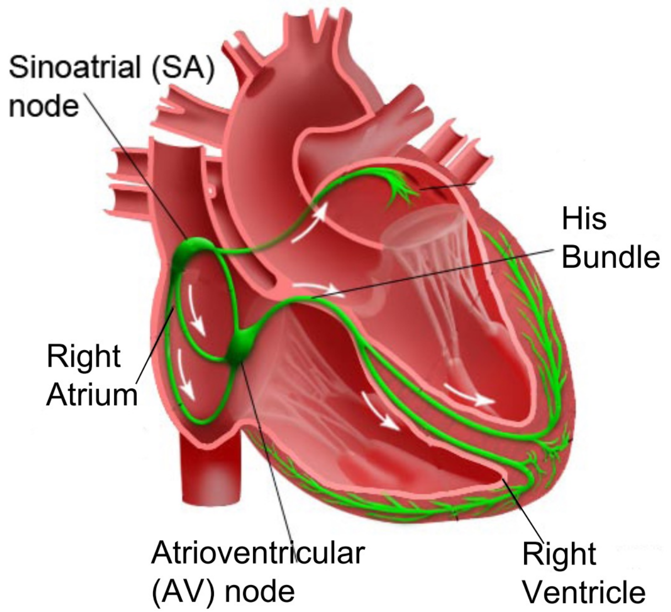


PaceMaker



Z. Jiang, M. Pajic, S. Moarref, R. Alur, R. Mangharam, *Modeling and Verification of a Dual Chamber Implantable Pacemaker*, In Proceedings of Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.

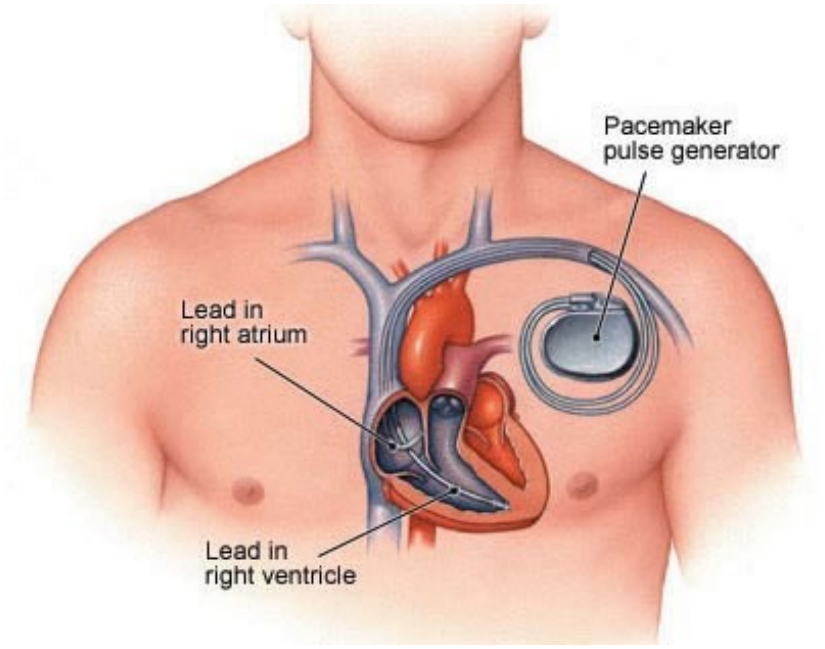
How does a healthy heart work?



- SA node (controlled by nervous system) periodically generates an electric pulse
- This pulse causes both atria to contract pushing blood into the ventricles
- Conduction is delayed at the AV node allowing ventricles to fill
- Finally the His-Pukinje system spreads electric activation through ventricles causing them both to contract, pumping blood out of the heart

Z. Jiang, M. Pajic, S. Moarref, R. Alur, R. Mangharam, *Modeling and Verification of a Dual Chamber Implantable Pacemaker*, In Proceedings of Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.

PaceMaker

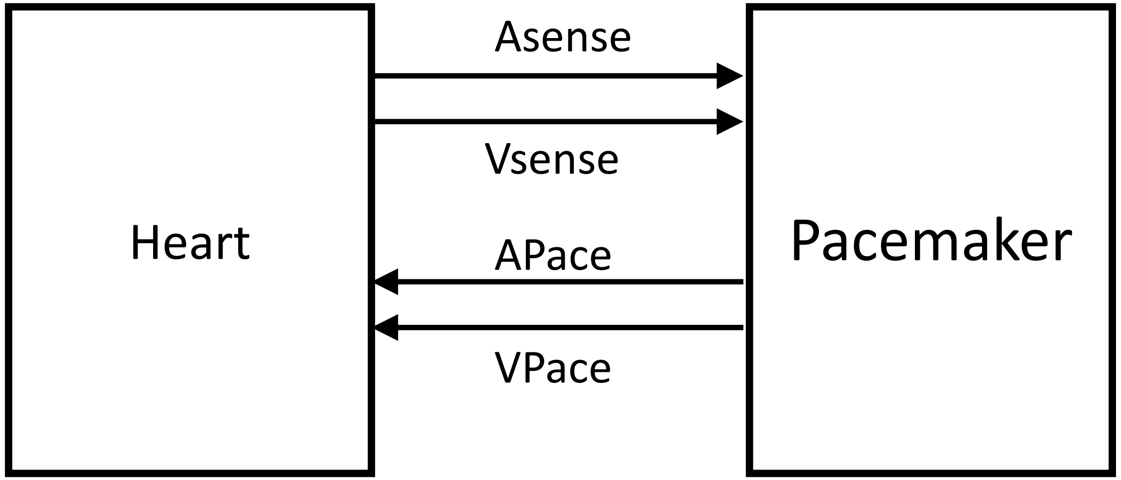


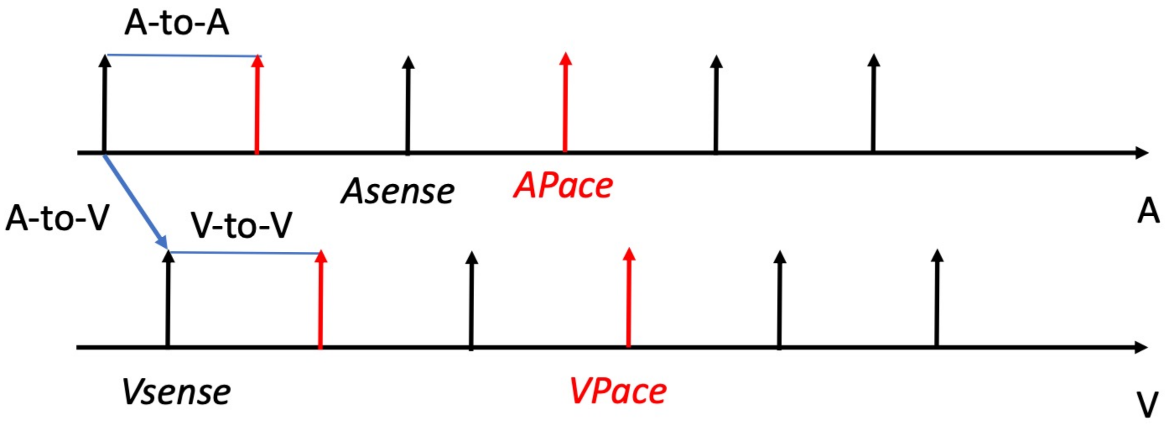
- Aging and/or diseases cause conduction properties of heart tissue to change leading to changes in heart rhythm
- Tachycardia: faster than desirable heart rate impairing hemo-dynamics (blood flow dynamics)
- Bradycardia: slower heart rate leading to insufficient blood supply
- Pacemakers can be used to treat bradycardia by providing pulses when heart rate is low

How dual-chamber pacemakers work

- Activation of local tissue sensed by the leads (giving rise to events Atrial Sense and Ventricular Sense)

- Atrial Pace or Ventricular Pace are delivered if no sensed events occur within deadlines

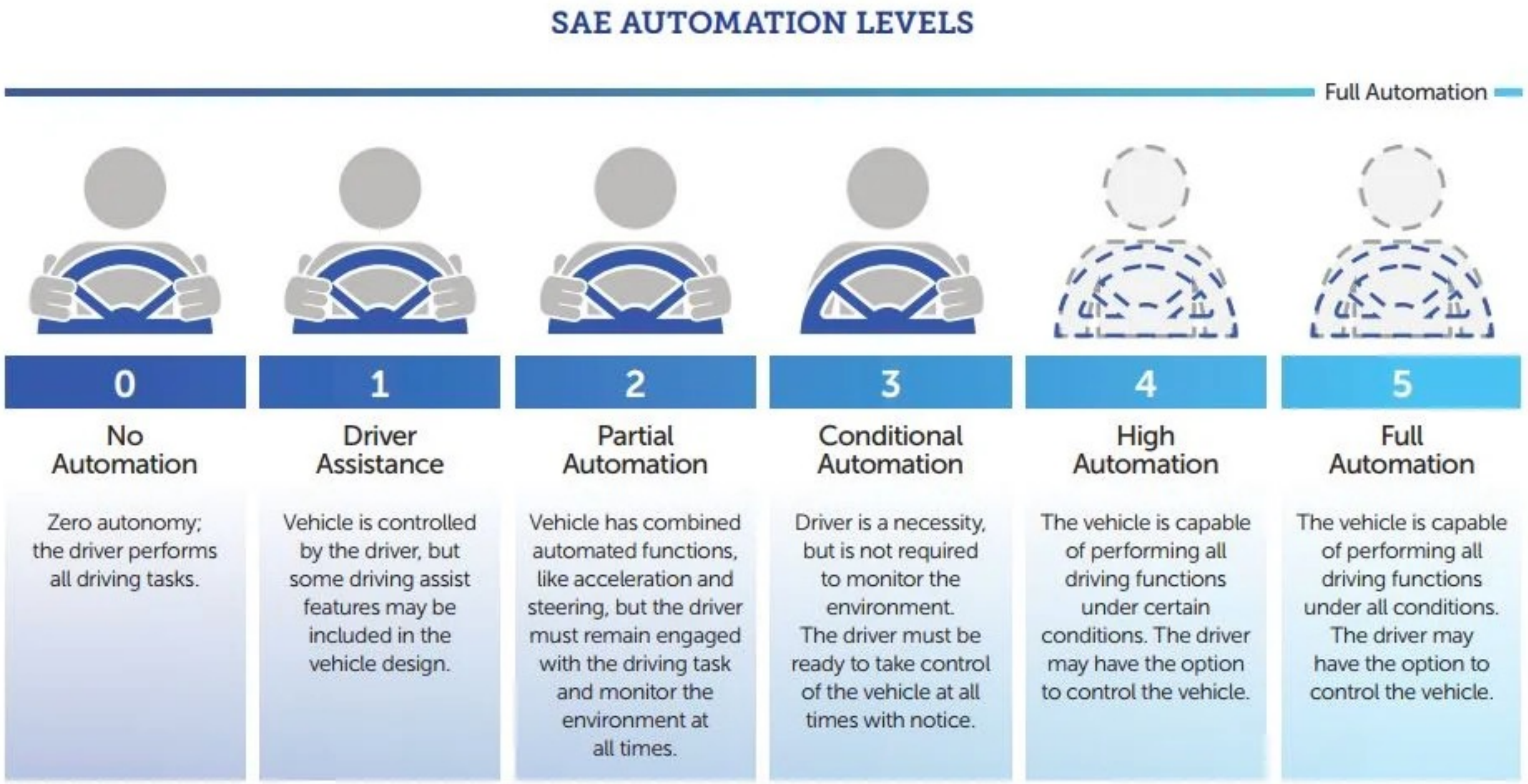




Transportation CPS

Everything that moves will become autonomous

Automotive Car

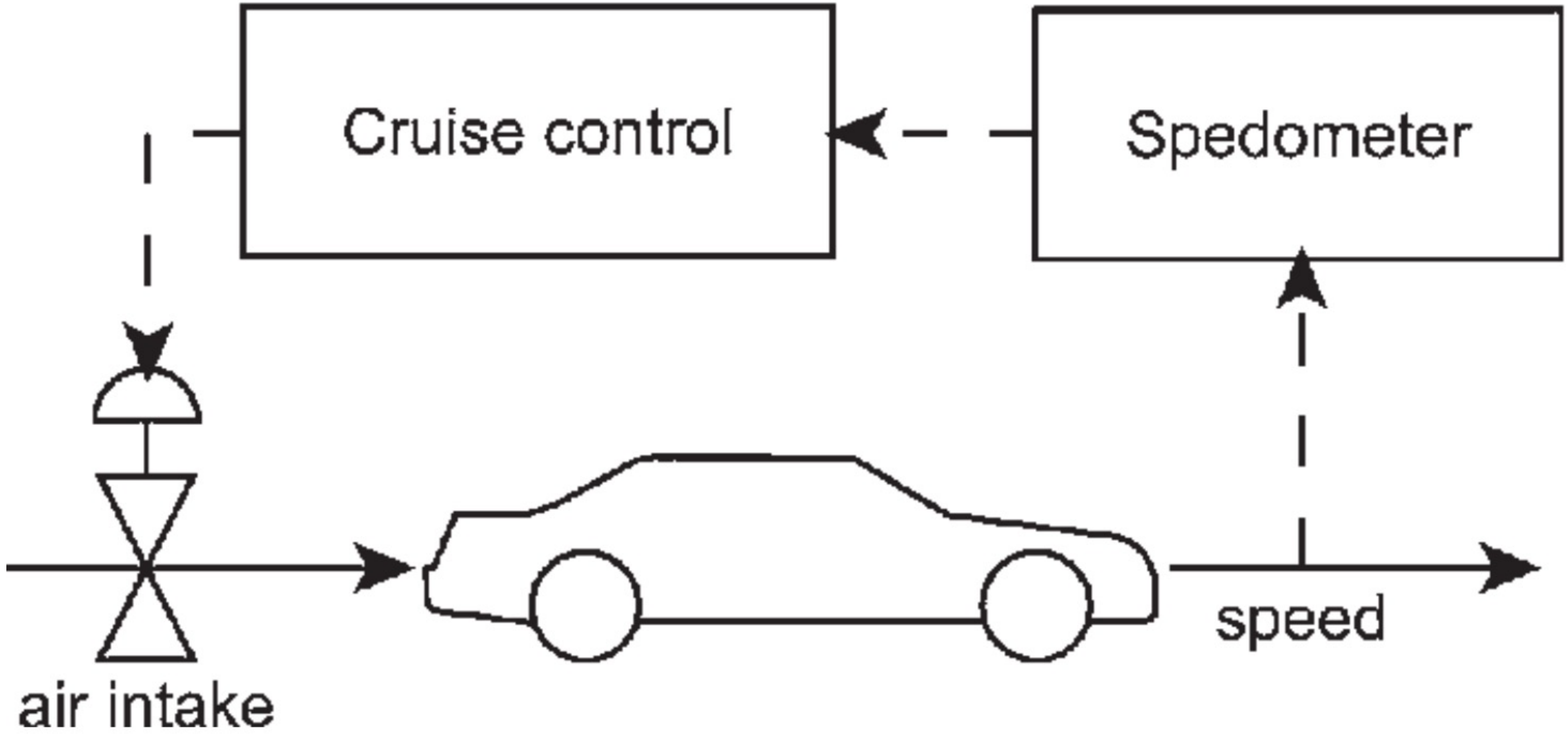


SAE AUTOMATION LEVELS

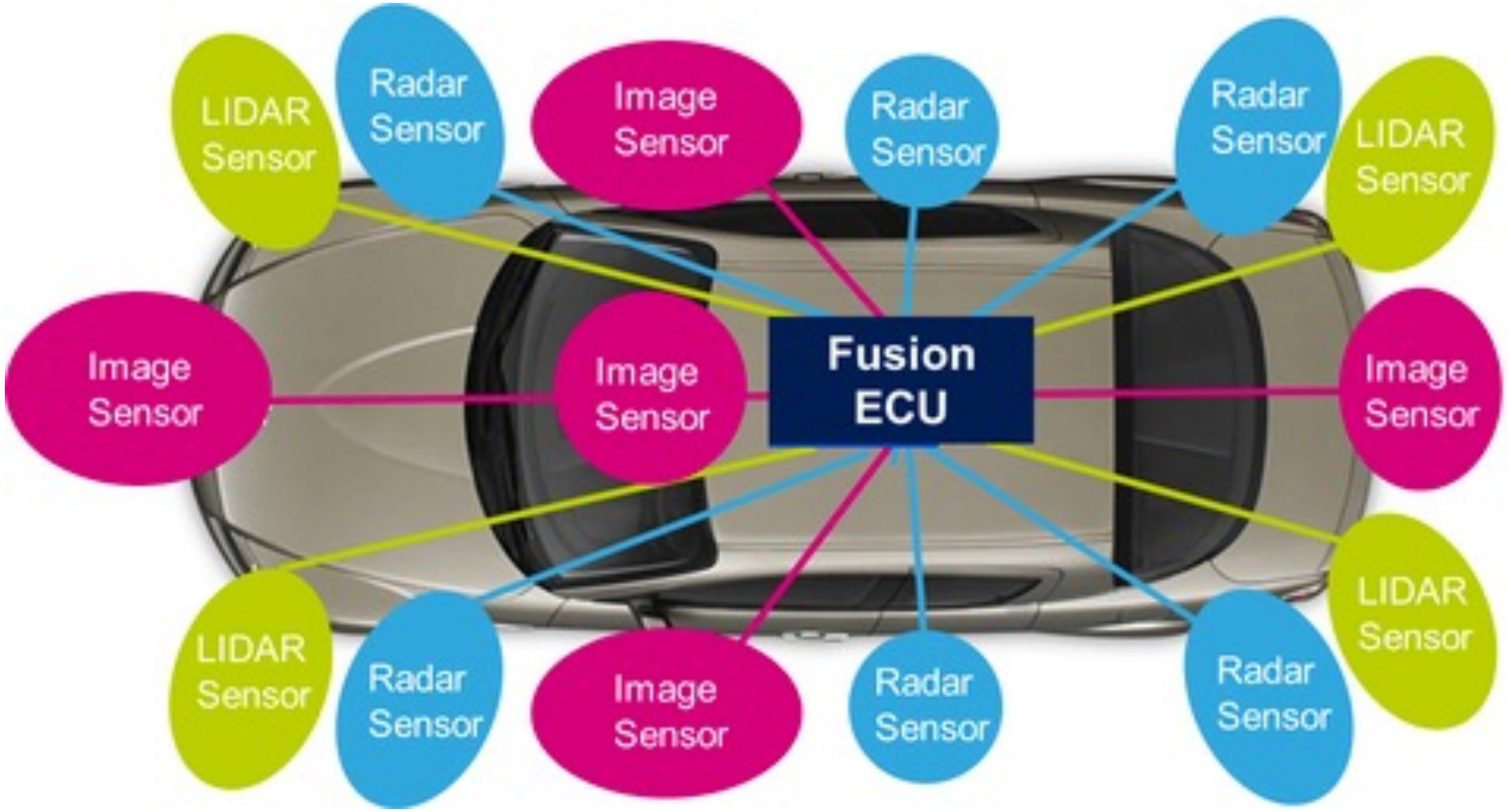
Full Automation

0	1	2	3	4	5
No Automation	Driver Assistance	Partial Automation	Conditional Automation	High Automation	Full Automation
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

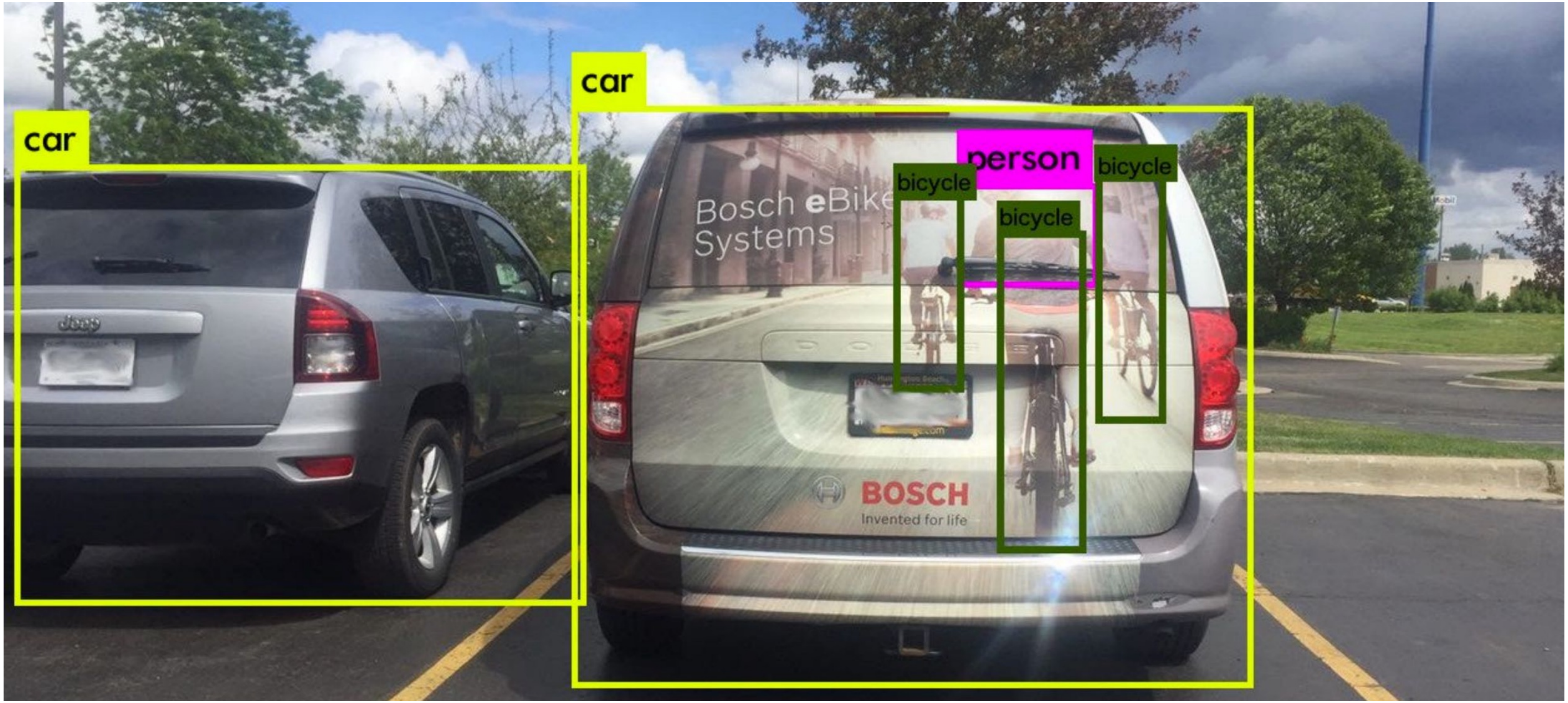
Automotive Car



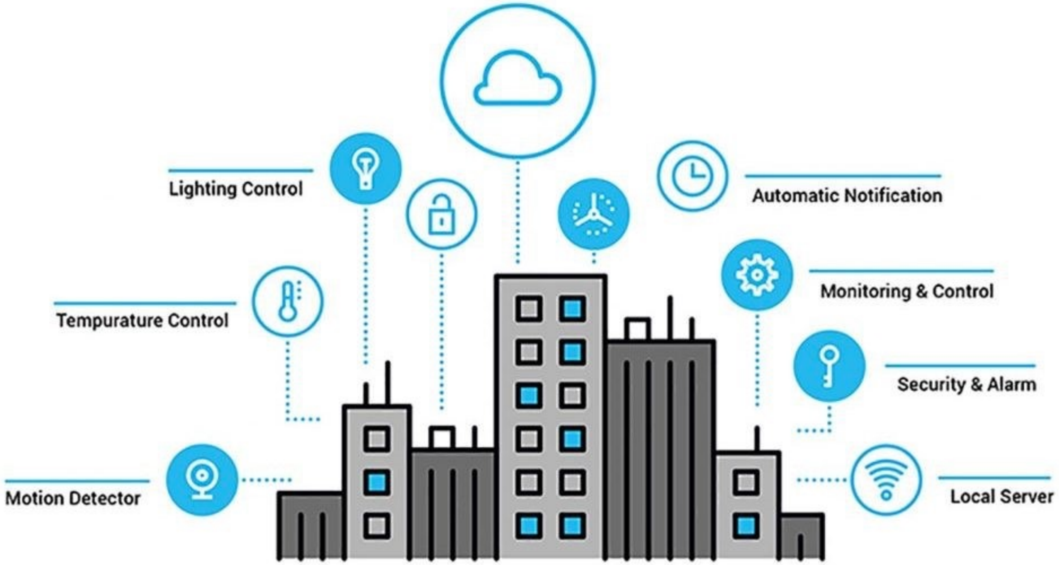
Automotive Car



Automotive Car

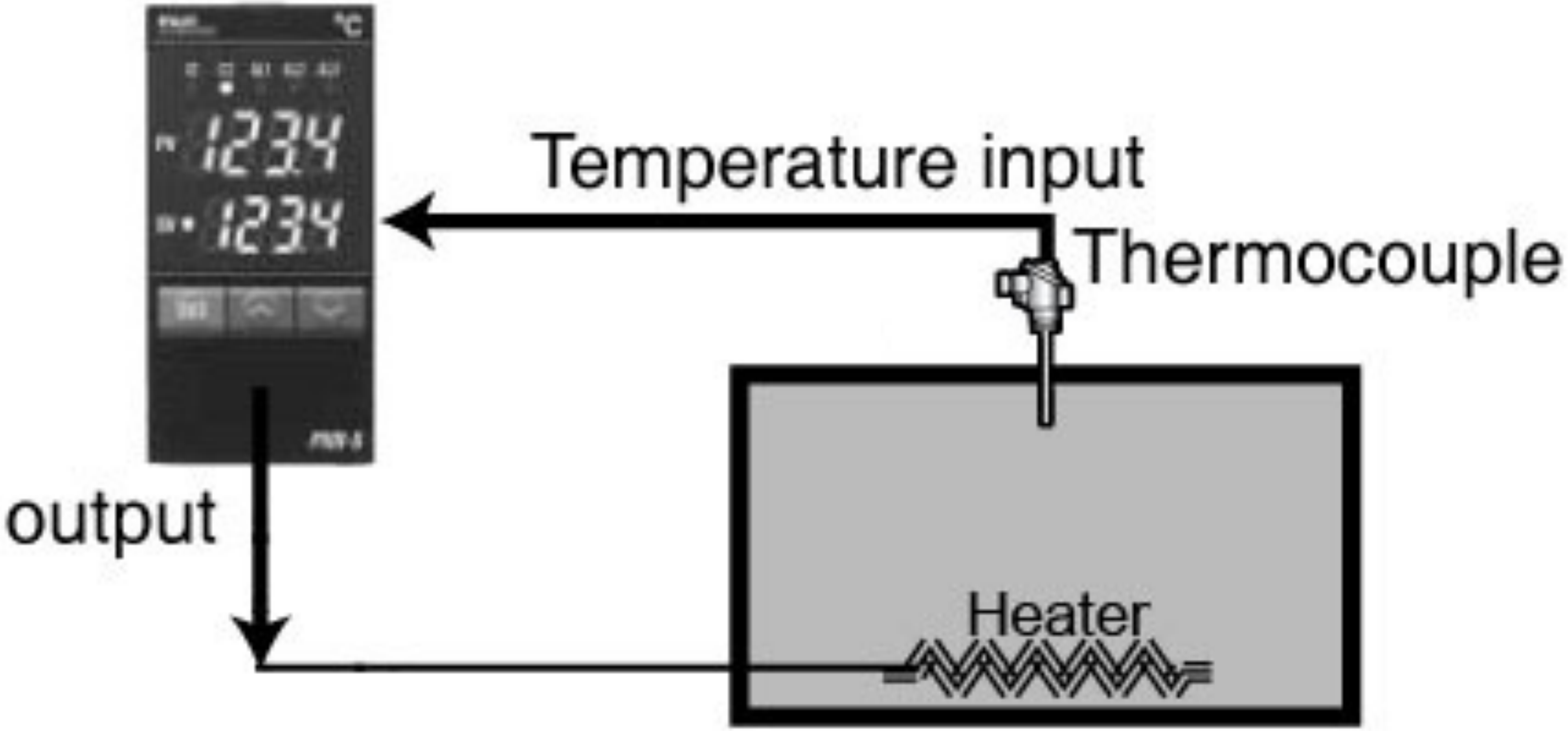


Energy

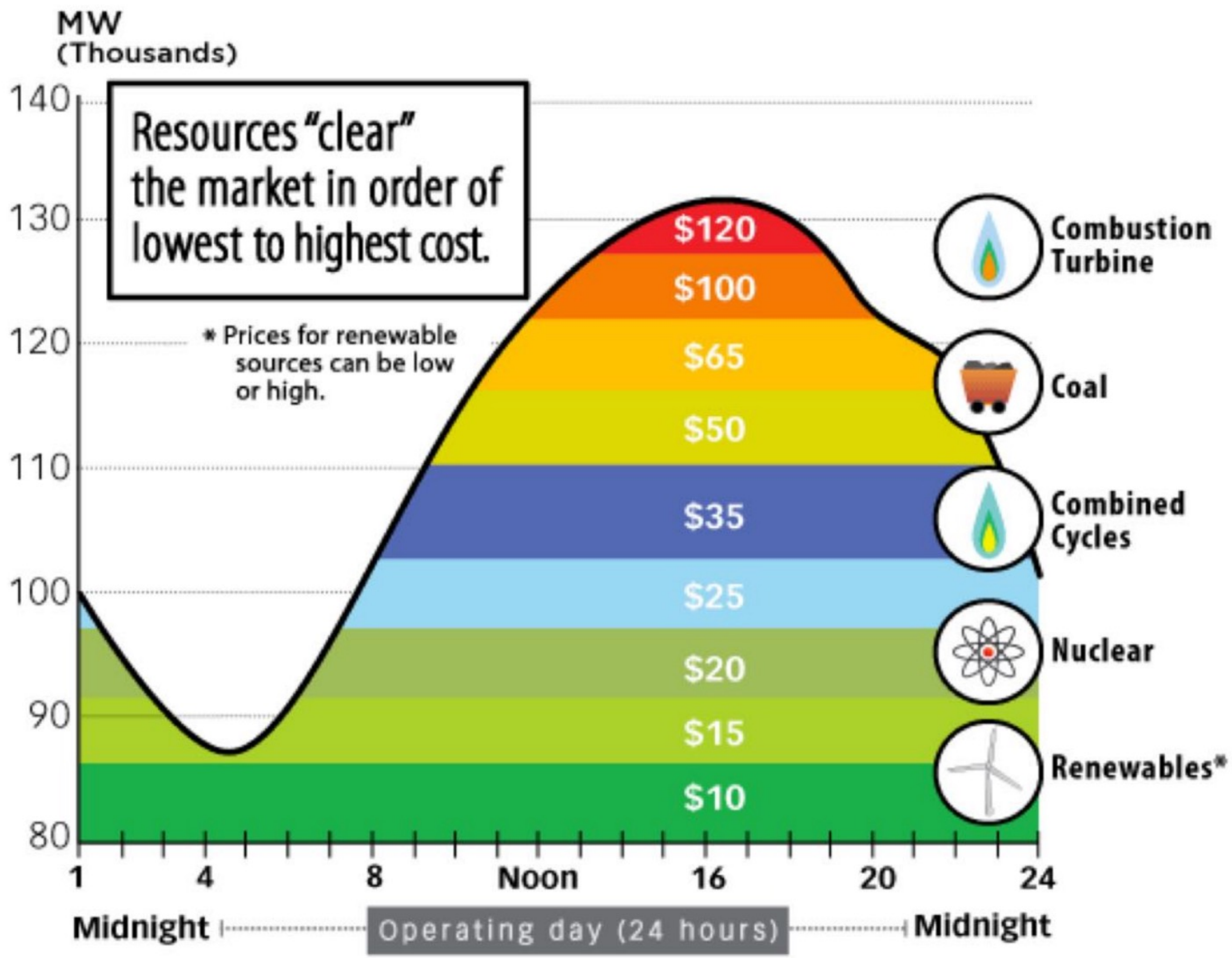

Lighting Control
Automatic Notification
Monitoring & Control
Tempurature Control
Security & Alarm
Motion Detector
Local Server

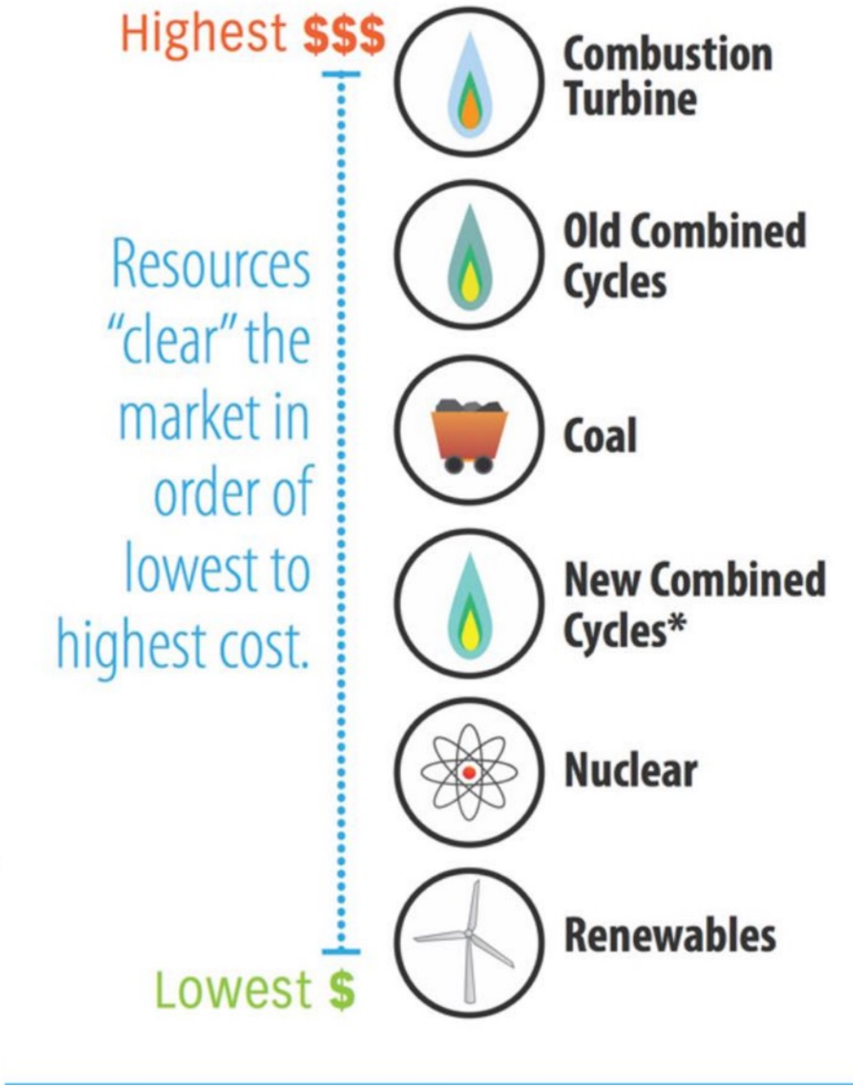
© Siemens

Temperature Control



Energy Control





even-thermostats-have-a-heart